PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE COMUNICACIÓN, LINGÜÍSTICA Y LITERATURA
ESCUELA MULTILINGÜE DE NEGOCIOS Y RELACIONES INTERNACIONALES

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE LICENCIADA MULTILINGÜE EN NEGOCIOS Y RELACIONES INTERNACIONALES

CIBERDEFENSA EN EL ESTADO ECUATORIANO PERÍODO 2013-2016

NORA CRISTINA SALINAS ABAD

DIRECTORA: Mtr. GILDA GUERRERO

FEBRERO, 2018
QUITO – ECUADOR

DEDICATORIA

Para Nora, Julio, Adrián, Pablo, Rafael y Matías, quien me inspira.

AGRADECIMIENTO

A mis amigos por compartir el viaje, a Gilda por las largas conversaciones y el conocimiento compartido, a Andrés Delgado Ron y a Byron Zamora que contribuyeron a esta investigación mediante las entrevistas.

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

I. TEMA

CIBERDEFENSA EN EL ESTADO ECUATORIANO PERÍODO 2013-2016

II. RESUMEN

Sobre la base de diferentes concepciones de seguridad vinculadas con el ciberespacio, la investigación tiene como principal propósito de estudio, analizar en su conjunto el área de gestión en materia de ciberdefensa desarrollada en Ecuador, en un período que comprende desde el año 2013 al primer semestre del año 2016; bajo diferentes parámetros que incluyen el punto de vista institucional, técnico, político y legal, que demanda el concurso de varios actores y escenarios. La estructura configurada será abordada a través del caso de la vulnerabilidad del Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE) que pertenece a la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt). Este estudio, se analiza con la clasificación del agente de amenaza y el objetivo del caso, además, desde el seguimiento institucional de las entidades públicas que intervinieron en la investigación. Las perspectivas de la Interdependencia Compleja y la Modernidad Líquida se encuentran inmersas en el trabajo. Los hallazgos muestran que la reflexión local no responde a la estructura internacional y que se requiere potencializar la institucionalidad.

Palabras Clave: Seguridad integral, ciberdefensa, Ecuador, interdependencia compleja, modernidad líquida, Senescyt.

III. ABSTRACT

Based on different conceptions of security related to cyberspace, the main purpose of this research is to analyze the cybersecurity management area developed in Ecuador in a period ranging from 2013 to the first semester of the year 2016; under different parameters that include the institutional, technical, political and legal points of view, which demands the participation of several actors and scenarios. The configured structure will be addressed through the case of the vulnerability of the National Higher Education Information System of

Ecuador (SNIESE) belonging to the Secretariat of Higher Education, Science, Technology and Innovation (Senescyt). This study is analyzed along the classification of the agent of threat and the objective of the case, in addition, it is analyzed from the institutional follow-up of the public entities that intervened in the investigation. The perspectives of Complex Interdependence and Liquid Modernity are embedded in the work. The findings show that local reflection does not respond to the international structure and that it is necessary to strengthen institutionalism.

Integral security**,** cyber-defense, Ecuador, complex interdependence, liquid modernity, Senescyt.

IV. RESUMÉ

Basé sur différentes conceptions de la sécurité liées au cyberespace, l'objectif principal de cette recherche est d'analyser la zone de gestion de la cybersécurité développée en Equateur dans une période allant de 2013 au premier semestre de l'année 2016 ; sous différents paramètres qui incluent le point de vue institutionnel, technique, politique et juridique, qui exige la participation de plusieurs acteurs et scénarios. La structure configurée sera abordée dans le cas de la vulnérabilité du Système national d'information sur l'enseignement supérieur équatorien (SNIESE) appartenant au Secrétariat de l'enseignement supérieur, de la science, de la technologie et de l'innovation (Senescyt). Cette étude est analysée avec la classification de l'agent de la menace et l'objectif de l'affaire, en plus, du suivi institutionnel des entités publiques qui sont intervenues dans l'enquête. Les perspectives de l'interdépendance complexe et de la modernité liquide sont intégrées dans ce travail. Les résultats montrent que la réflexion locale ne répond pas à la structure internationale et qu'il est nécessaire de renforcer l'institutionnalité.

Sécurité intégrale, cyberdéfense, Ecuador, interdépendance complexe, modernité liquide, Senescyt.

V. INTRODUCCIÓN

La incorporación de las Tecnologías de la Información y de la Comunicación en la vida cotidiana de los Estados, ha generado un escenario que facilita el desarrollo de redes que permiten el intercambio de información y la interacción de la ciudadanía y las funciones del Estado; no obstante, al mismo tiempo, se presentan amenazas que pueden afectar la seguridad nacional. Dentro de este marco, Ecuador desde al año 2008 ha incorporado el concepto de seguridad integral para la conducción política y estratégica del Estado en nuevos dominios que se conforman. Así, entra en debate el término ciberdefensa y la configuración de su estructura. La hipótesis central que se plantea sobre la problemática se dirige a responder que las vulnerabilidades de la ciberdefensa en Ecuador, en el período 2013-2016, tendrían origen en la falta de medidas jurídicas, institucionales y técnicas desde el mismo Estado ecuatoriano; que evidenciaría la ausencia de seguridad en la información estatal.

El objetivo principal de la investigación propone analizar la vulnerabilidad de la seguridad informática ante las nuevas tecnologías y sus efectos colaterales; determinando las principales causas para establecer políticas internas que regulan la seguridad informática nacional, demostrando el impacto de las filtraciones y delitos informáticos en Ecuador y las falencias de la estructura de las regulaciones y reglamentos que existen sobre seguridad informática. El fundamento teórico se basa en dos enfoques, distintos pero complementarios. En primera instancia, se considera a la teoría de la interdependencia compleja propuesta por Robert Keohane y Joseph Nye, debido a que comprende temas como los múltiples canales que conectan a las sociedades, entre los que se ha identificado el "ciberespacio" así mismo, considera nuevos temas como la tecnología dentro de las agendas de los Estados y la interacción de las instituciones dentro de la era de la información. En segunda instancia, la modernidad líquida planteada por Zygmunt Bauman propone el tema de la "fluidez" que está asociada al tema de la información que fluctúa a través de las diferentes herramientas tecnológicas, además, propone el alcance del tiempo y espacio por medio de recursos, donde la información llega a ser la fuente de poder.

Bajo los anteriores parámetros, el primer capítulo de la disertación se presenta como una sección destinada al análisis de los cambios conceptuales y aproximaciones teóricas sobre seguridad que se han venido construyendo a lo largo de los años para responder a una de las demandas de los habitantes, y, de acuerdo a la visión de los Estados con respecto a la protección que deben a sus ciudadanos dentro del territorio; y a la par, de los grandes acontecimientos externos que pueden afectar a la soberanía de sus fronteras o incidir en la opinión o comportamiento político, económico, social, ideológico o cultural del país. Así pues, estos temas recaen en la vulnerabilidad de la seguridad por la presencia de amenazas de diverso orden. Como resultado de la evolución de las opiniones vertidas se llega a formular el concepto de seguridad integral o seguridad pública. En consecuencia, en materia de seguridad, se debe analizar por separado, es decir, desde el punto de vista del individuo, del Estado y de las políticas internacionales que gravitan en el orden mundial.

Por otra parte, con la revolución tecnológica y la globalización, el propósito de este capítulo es comprender el significado y el alcance del término ciberespacio e indagar los escenarios en donde se gesta y se desempeña el tema de la ciberdefensa estatal. Es cuando, en materia de seguridad los Estados tienen un nuevo desafío coyuntural, como es el impulsar un proceso de modernización tecnológica a pasos agigantados que llevaría a obtener cierto grado de soberanía sobre este nuevo dominio global interactivo en torno a la información. En este ámbito, la seguridad se vuelve vulnerable por las múltiples posibilidades de amenazas y/o ataques que pueden representar un peligro de desestabilización del Estado y sus ciudadanos; entonces, surgen nuevos términos como ciberdelito, ciberespionaje, ciberterrorismo y ciberguerra. Se considera también, la preocupación de los Estados por el internet asociado al ciberespacio que conlleva a discutir temáticas como la infraestructura de acceso, los derechos de privacidad de los individuos mediante leyes a su favor, como también, las regulaciones y aplicaciones tecnológicas que emanan del Estado, que pudieran atentar a la libertad de los individuos al interactuar por las redes.

El segundo capítulo, en materia de ciberdefensa y para mayor comprensión del tema en el caso ecuatoriano, se sintetiza con el análisis histórico del camino

recorrido, en el cual en sus inicios se destaca la primacía militar en todos los aspectos de seguridad, enfocados a la defensa territorial; como también la evolución de los conceptos de seguridad y defensa que conducen en primer término a modificar en 1979 la Ley de Seguridad Nacional, que amplía la visión de seguridad tomando aspectos socio económico y cultural. Es importante recordar que el país ha permanecido inmerso en conflictos bélicos con su país vecino, el Perú, hasta la firma de la Paz en 1998, así como los hechos que se suscitan en la frontera norte, por lo tanto, la seguridad estaba comandada por las Fuerzas Armadas con mínima participación del Ejecutivo y Legislativo.

Más adelante, la inestabilidad política, conduce a diseñar la "Agenda de Defensa Nacional 2005-2006", con nueva planificación y la actualización del Libro Blanco para consolidar la relación civil-militar, que añade aspectos de los refugiados y desplazados del conflicto colombiano. Además, los acontecimientos suscitados el 11 de septiembre de 2001 en los Estados Unidos, inciden directamente en las políticas internas del país, que obliga a implementar políticas para combatir el terrorismo y la violencia organizada como amenaza. Sin embargo, no es hasta la vigencia de la Constitución de 2008, cuando se da un giro en esta materia para asumir como -seguridad integral- con el rol preponderante del Estado, con la aprobación de leyes como un hecho concreto en el ámbito político-administrativo, y la creación de organismos con este propósito, vinculado al Plan Nacional del Buen Vivir (2013-2017), la Ley de Seguridad Pública y del Estado (2009), y se desarrolla en el Plan Nacional de Seguridad Integral (2011-2013).

Posteriormente, en 2014 se actualiza el Plan Nacional de Seguridad Integral (2014-2017) y se inicia el debate y análisis de los conceptos de ciberdefensa, ciberseguridad, ataques cibernéticos y el concepto político de las "guerras cibernéticas", relacionados con la evolución tecnológica y científica. Se responsabiliza a las Fuerzas Armadas y al Ministerio de Defensa Nacional, mediante la creación del Sistema de Ciberdefensa. De lo anotado, se desprende que en materia de seguridad el Estado ecuatoriano ha logrado varios cambios en sus planes de seguridad, que en cierta medida se ajustan a la evolución del concepto de seguridad integral, al amplio espectro de amenazas y a la globalización de los problemas en este tema y quizá lo más importante es la

institucionalidad para enfrentar la protección de los ciudadanos (el ser humano como fin prioritario) y la defensa de la soberanía nacional, implementado como política de Estado. Así mismo, se considera el avance en el marco jurídico e infraestructura, no obstante, pese a los esfuerzos dirigidos en este campo persisten la existencia de vulnerabilidades.

Derivado de lo anterior, en el estudio se analiza varios elementos complementarios que se vinculan al concepto y la estructura del ciberespacio y de la ciberseguridad, entre los que se destacan la gobernanza de internet y los varios tópicos que se derivan en cuanto a infraestructura, acceso y uso en el período 2013-2016. Igualmente, estos temas han sido analizados tanto en el ámbito global tomando en cuenta la dependencia tecnológica y en la Unión de Naciones Suramericanas (Unasur) se discuten temáticas concernientes a seguridad nacional y regional, estos contenidos facultan comprender la dimensión en la cual se aplica la ciberdefensa y la ciberseguridad.

Correspondiente al capítulo tres, la revisión y análisis de los casos de instituciones ecuatorianas que fueron blanco de ataques cibernéticos, conducen a descifrar sobre los intereses que mueven a los agentes de amenaza, por una parte, y por otra, dan fe de la vulnerabilidad de los sistemas informáticos, que dejan al descubierto o manipulan información en desmedro de organismos públicos, privados y la intimidad de los individuos.

Así también, las revelaciones en 2013 realizadas por Edward Snowden que formaba parte de la Agencia de Seguridad Nacional (NSA), de documentos de inteligencia de los Estados Unidos, demostraron la vulnerabilidad de los sistemas de ciberseguridad y defensa, sucesos que alertaron al ámbito internacional. En el caso ecuatoriano, sus instituciones sufrieron ataques cibernéticos durante el período 2013-2016 y se presentan los casos más representativos, con el objetivo de medir el alcance que tienen los delitos cibernéticos. Pero además, se analiza el caso de estudio la vulnerabilidad del Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE) perteneciente a la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt) y, que

corresponde al último trimestre de 2015 e inicios del 2016 como cierre del período de investigación.

Para este hecho, se analiza la vulnerabilidad del sistema utilizando la clasificación del Criptológico Nacional- CERT de España (2016), con el fin de identificar los agentes de la amenaza y objetivos en el desarrollo de la operación cibernética, además del seguimiento de las instituciones que intervinieron en base a la propuesta de Choucri, Madnick y Koepe. El objetivo de la tabla permite medir a través de datos cuantitativos y cualitativos el desempeño de la organización. Para terminar, cabe enfocar los términos de globalización, interdependencia compleja y modernidad líquida, relacionada con la expansión tecnológica y sus canales de comunicación desde el punto de vista de la naturaleza del ciberespacio.

En términos generales, el aporte de la carrera Multilingüe en Negocios y Relaciones Internacionales a la disertación se ve reflejado en los estudios interdisciplinarios de las asignaturas. La investigación se desarrolla en el eje temático de la seguridad y conflicto, en el contexto en que las relaciones de los diversos actores del sistema internacional, generan amenazas multidimensionales de toda índole, en este caso cibernéticas y, que tienen influencia directa con la seguridad del aparataje estatal. Así mismo, es un estudio que requiere abarcar temáticas sobre política exterior, ciencias políticas, realidad latinoamericana, entorno mundial contemporáneo y derecho. Por lo tanto, la disertación se encuentra inmersa en la carrera, pues contribuye a formar investigaciones que aporten a la realidad local e internacional desde un enfoque multidisciplinario.

CAPITULO I
EL CONCEPTO DE SEGURIDAD Y LA CIBERDEFENSA ESTATAL

1.1. Las variaciones del concepto de seguridad

La seguridad es un concepto que a partir del lenguaje de las ciencias sociales ha sido explorado desde diferentes perspectivas y que, además, al delimitar su significado se han empleado distintas corrientes teóricas, aunque aún es objeto de un profundo debate por alcanzar un consenso, su valor adquiere varias formas en función de factores endógenos y exógenos que caracterizan un Estado. De ahí, la importancia de destacar que las definiciones que se pueden obtener se evidencian en las diversas variantes en las que se presenta, puesto que tiende a ser un concepto que evoluciona de acuerdo a la construcción social y estatal, de esta manera se puede mencionar tipos como: nacional, humana, multidimensional, integral, cooperativa, entre otras (Laborie, 2011).

A pesar de existir múltiples disimilitudes, la discusión va más allá de la materia académica, la concepción teórica influye en varios aspectos como en lo político, en la toma de decisiones y en el ámbito militar. (Vanella, 2015). Aunque en otros casos la seguridad llega a ser un concepto utilizado para justificar diversos hechos desde la suspensión de libertades civiles hasta el inicio de actividades bélicas (Baldwin, 1997). Al intentar comprender el significado se interponen diferentes ideas y términos que se relacionan cuando se analiza la seguridad, y al ser igualmente una palabra cargada de ideologías se puede direccionar en numerosos ámbitos.

Por lo expuesto, el presente apartado aborda la conceptualización de la seguridad, además, de dos definiciones fundamentales que forman parte de las dinámicas de la construcción del concepto entorno al sistema y los Estados, el caso de las definiciones de seguridad nacional y seguridad humana; a la par, se analiza al final del subcapítulo la seguridad integral como un concepto que se ha extendido en la agenda de los Estados latinoamericanos.

1.1.1. Conceptualización y re conceptualización de la seguridad

Para aproximarse a las variaciones del concepto de seguridad es fundamental en primer lugar establecer el significado de seguridad. En el discurso político no se desarrolla de manera profunda, es ahí donde surge uno de los problemas para la comprensión de los conceptos actuales de seguridad y de las contradicciones que puedan presentarse (Cubides & Garay, 2013). El concepto de seguridad responde a las lógicas de los actores que lo utilizan y es de importancia señalar que se pueden encontrar multiplicidad de significados. El término seguridad es un concepto que por su dinamismo puede generar confusión o dificultad al determinar su definición.

Para comprender el concepto de seguridad, éste debe analizarse desde una visión flexible puesto que existe una reformulación constante por parte de los Estados y sus interpretaciones. Además, la seguridad se encuentra estrechamente relacionada con otras ciencias y disciplinas e influye de manera directa en la creación de sistemas, formulación de políticas, leyes y doctrinas (Muñoz, 2005). La seguridad no es un concepto independiente, está relacionado con valores individuales, culturales, sociales y en sí sistémicos. La seguridad entonces es intersubjetiva debido a que es el resultado de un proceso de interacción y negociación (Schäfer, 2012).

Con el objetivo de no caer en la estandarización del concepto y siguiendo a David A. Baldwin (1997), para quien, los conceptos especialmente controvertidos están cargados de valor y que los argumentos y evidencias no conducen a un solo "uso correcto"; se analizan diferentes variantes con el propósito de ir discutiendo sobre la conceptualización de la seguridad y obtener una visión amplia.

La discusión comienza por definir el concepto sin ninguna especificación, que puede llevar a que se caiga en la ambigüedad. De hecho, en términos generales la palabra seguridad según La Rotta (2002) "se origina del latín secur-tas, la cual se deriva del adjetivo -securus- que en su sentido más general significa estar libre de cuidados*"* (Cubides & Garay, p.84*).* Por otra parte, la caracterización de la

seguridad de Arnold Wolfers (1952) expresa: "La seguridad, en un sentido objetivo, mide la ausencia de amenazas a los valores adquiridos, en un sentido subjetivo, la ausencia de temor de que tales valores sean atacados"[1]. Para Barry Buzan (1991, p.18) "la seguridad es la búsqueda de la libertad de la amenaza (…)"[2]. Estas definiciones en una primera percepción hacen que su comprensión se torne compleja, sin embargo, capturan los elementos del uso del concepto de seguridad.

En esta problemática se puede considerar el análisis comparativo que no tiene como propósito formular una nueva definición integral, más bien encontrar elementos en común para su análisis (Šulović, 2010). Dentro de este contexto, se analizan los siguientes términos: el objeto de la seguridad, los valores y la amenaza. En cuanto al objeto, Buzan (1991) específica que existen tres niveles en los que se direcciona la seguridad: los individuos, los Estados y el sistema internacional. Estos niveles están estrechamente relacionados y para comprender las dinámicas se debe entender cada sector para conocer la influencia que ejercen entre sí (Stone, 2009). De este modo, se abordan los objetos con una metodología macro y micro, considerando que la seguridad es un concepto que ha ampliado sus límites extendiéndose de los asuntos estatales (Møller, 1996).

Por otra parte, el término amenaza surge simultáneamente cuando se tiene en mente la palabra seguridad. Es por ello que Jean (2007), incluye en el concepto la percepción de las amenazas. Es decir, que se extiende el significado a la existencia o no de que la intención hostil se materialice (Bartolomé, 2004). Igualmente, viene al caso señalar la definición de amenaza planteada por Richard H. Ullman (1983, p.133) "es una acción o secuencia de eventos que amenazan drásticamente y durante un lapso de tiempo relativamente breve para degradar la calidad de vida de los habitantes de un Estado, o amenaza significativamente con reducir el abanico de opciones políticas disponibles para el gobierno (…)"[3]. En este punto, además, cabe agregar el concepto de vulnerabilidad desarrollado por Keohane y Nye sobre el efecto de hechos externos y la capacidad de reducirlos

[1] Traducción de la autora
[2] Traducción de la autora
[3] Traducción de la autora

(1989). Entonces, los actores reaccionan de manera distinta a las amenazas en base a sus percepciones y recursos (Malec, 2003).

En cuanto a los valores, se debe señalar que los individuos, los Estados y otros actores sociales incluyen valores físicos, económicos, de bienestar, de autonomía entre otros. Tradicionalmente se han incluido valores como la independencia política e integridad territorial. La necesidad de detectar nuevos valores origina que el concepto considera temas enfocados en los derechos humanos como el hambre, las enfermedades y las libertades individuales e incluye temas del *modus vivendi* cotidiano (Bartolomé, 2004). En el caso de Wolfers (1952) que utiliza la objetividad y la subjetividad dentro del término seguridad hace referencia a la probabilidad de generar daño a los valores, como por ejemplo en la dimensión subjetiva donde podría el Estado percibirse seguro a pesar de que no lo es (Baldwin, 1997).

Este concepto complejo requiere una mirada amplia que vaya más allá de lo general, considerando otros elementos adicionales que inciden en el concepto como son los costos. Desde este punto de vista, en la búsqueda de la seguridad existen recursos que son empleados en el mantenimiento militar, la promoción de la tranquilidad pública y otros relacionados con el ambiente del individuo. No obstante, dentro de la política de seguridad también se han sacrificado otros valores en aras a la seguridad, donde se abordaría a un tema más complejo como es el de la moral (Baldwin, 1997).

Por consiguiente, el concepto de seguridad se está ampliando a diferentes campos y temas, así como a múltiples dimensiones que se han vinculado al concepto; sin embargo, todavía no existe un consenso sobre los límites que debería alcanzar (Møller, 1996). En efecto, al avanzar en la expansión del significado según Ole Wæver (1998) el concepto puede entrar en el término de la "securitización"[4] es decir, elevar a la seguridad todos los problemas. La

[4] En concordancia con Gabriel Orozco (2006: 145), el término de la "securitización" se establece como un proceso mediante el cual se pretende darle calidad o estatus de asunto de seguridad a un problema que puede atentar contra la supervivencia de un ente, ya sean individuos, conglomerados, Estados o la humanidad. Este vocablo proviene del inglés securitization. Se utiliza la palabra seguritización y el verbo

"securitización" siguiendo a Buzan (1998, p.31) "es intersubjetiva y socialmente construida: un objeto referente sostiene la legitimidad general como algo que debería sobrevivir, lo cual torna necesario que los actores puedan referirse a él, apuntando a algo como una amenaza". Por lo tanto, en el discurso político se puede declarar cualquier tema como un "problema de seguridad", e igualmente la situación podría influir en el abuso de prohibiciones de ciertos asuntos y a la separación de oponentes ideológicos. Esta expansión del concepto surge en general en el discurso político de los actores securitizadores, que definen los objetos y la percepción de amenazas (Møller, 1996).

Efectivamente, después de analizar los diversos cambios conceptuales de la seguridad, es fundamental analizar aspectos importantes para una determinada comunidad, al contrario de homogeneizar el sistema internacional, siguiendo a Buzan et al (1998, p.164) "A pesar de la estructura global general, hay diferencias regionales que son demasiado cruciales para ser desatendidas". Las dinámicas de la seguridad y la interacción que existe entre los diferentes actores estarán también condicionadas por la interdependencia que exista entre ellos (Orozco, 2006).

Al limitar el concepto de seguridad al nivel estatal o extender el término hacia el individuo, considerar los diversos temas que se encuentran en la agenda de los Estados y analizar factores particulares de cada concepto; se concluye que las todas definiciones son válidas y algunas pueden ser más útiles que otras. A continuación, se separan a los autores en base a sus conceptualizaciones y tendencias teóricas.

seguritizar como una licencia académica, pues es un neologismo utilizado en los estudios de seguridad que no tiene traducción oficial al español.

TABLA 1

AUTORES Y TEORÍAS DESDE EL CONCEPTO DE SEGURIDAD

Autor	**Tendencia**	**Objeto referente**	**Argumentación**
Arnold Wolfers	Realismo	Estado	Los intereses nacionales se conciben dentro de la interpretación de la seguridad nacional, la protección a través del poder es la habilidad de controlar las acciones de otros Estados.
Richard Ullman	Neorrealismo	Estado	El concepto de seguridad nacional se profundiza, diversos eventos amenazan la calidad de vida de los habitantes, que afecta la estabilidad estatal y genera un cambio en la toma de decisiones.
Robert Keohane & Joseph Nye	Interdependencia Compleja	Sistema Internacional	La vulnerabilidad ante las amenazas externas permite la disponibilidad de alternativas para reducir las amenazas; sin embargo, implica también costos impuestos por los eventos externos y las acciones tomadas.
Elisabeth Jean	Interdependencia Compleja	Sistema internacional	Las amenazas deben enfocarse en el impacto de la estabilidad del Estado y como afecta a la seguridad de las naciones. En este sentido, deben incluirse los desafíos que enfrenta el sistema internacional.
Ole Wæver	Constructivismo	Sociedad	El concepto tradicional de seguridad nacional necesita expandirse e incluir dinámicas relacionadas con temas internacionales y subestatales. La securitización se forma en el discurso para considerar cualquier problema como una amenaza existencial.
Barry Buzan	Constructivismo	Sociedad	La definición de la seguridad puede aplicarse a diversos actores, no solamente los Estados sino también a los individuos. El concepto se expande a diversos sectores diferentes al militar.

Fuente: Wolfers, (1952); Wæver (1998); Buzan (1991); Ullman, (1983); Keohane & Nye, (1989).
Elaborado por: Cristina Salinas

1.1.2. El cambio de paradigma de la seguridad nacional a la seguridad humana

La diversidad de enfoques sobre la seguridad y las diferentes aproximaciones teóricas se orientan a considerar factores como los actores involucrados, entorno y período. En este marco, la seguridad dentro del debate de las relaciones internacionales se ha enfocado históricamente en las instituciones del Estado. La seguridad tradicionalmente y la mayor parte de la literatura está direccionada al análisis de los conceptos de poder y paz desde la perspectiva de la seguridad nacional (Buzan, 2008). De esta manera, partiendo desde las teorías clásicas de relaciones internacionales, la seguridad se analiza desde una noción realista y, desde el realismo estructural o neorrealismo.

Para empezar, y siguiendo la lógica expuesta en la sección anterior, es importante establecer el objeto referente de la seguridad, así, para el realismo y neorrealismo se trata de la integridad territorial del Estado (Orozco, 2006). De acuerdo con George F. Kennan (1948) el término de seguridad nacional es "la capacidad continuada de un país para proseguir el desarrollo de su vida interna sin interferencia seria, o amenaza de interferencia de potencias extranjeras" (Laborie, 2011). Para Kennan el predominio del realismo como pensamiento en el ámbito de la política exterior ha facultado que los Estados alcancen sus intereses (Martínez, 2005). De acuerdo a lo expuesto, los Estados utilizan y confían en el poder militar con el objetivo de neutralizar las amenazas de las fuerzas armadas de otros Estados. El efecto que tiene a nivel externo es de mantener la soberanía y el equilibrio de poder entre los países y en lo interno se protege los intereses nacionales. (Laborie, 2011).

Continuando con esta línea de pensamiento, Hans J. Morgenthau (1986) enfoca sus argumentos en el concepto de poder y sostiene que el desperfecto del mundo se debe a tres casusas: "el egoísmo y el deseo de poder de los hombres, los intereses nacionales de los Estados en términos de poder y la naturaleza anárquica del sistema". Desde la visión de Morgenthau, el Estado es el principal actor en el sistema internacional anárquico, en donde los Estados tienen como principal objetivo el poder. En el campo particularmente de la seguridad y en referencia a la política internacional, el factor militar como amenaza constituye el poder

político de una nación. Así, la idea de fuerza de un país se convierte en un instrumento para conseguir sus intereses, convirtiendo el tema militar en prioridad de los Estados (Cujabante, 2009).

Desde el punto de vista neorrealista o realismo estructural, la contribución de Waltz (1979, p.102) es explicada desde la anarquía estructural del sistema internacional en este sentido expone "(…) algunos Estados pueden en cualquier momento usar la fuerza, todos los Estados deben estar preparados para hacerlo – o vivir a merced de sus vecinos más vigorosos. Entre Estados, la naturaleza del Estado es el estado de guerra"[5]. Se evidencia que Waltz le asigna al Estado el rol principal, en un primer momento dirigido a la sobrevivencia en el sistema internacional para alcanzar sus intereses, con este objetivo es fundamental reunir recursos en el ámbito militar y disuasivo para garantizar la seguridad nacional (Álvarez, 2007). En este sentido, se comprende el énfasis que se otorga al aspecto militar por parte del Estado, como un elemento de protección de las diversas amenazas a la seguridad, donde existe la persistente lucha de los Estados por poder, en una atmósfera de anarquía.

Por otro lado, en concordancia con las diferencias regionales que explica Buzan (1998), en el contexto de América Latina se desarrolla la doctrina de seguridad nacional, este fragmento de la seguridad está condicionada con el *statu quo* de los países hegemónicos. En relación con ese tema, se debe citar a Edgar Velásquez (2002, p.11) quien define como "la sistematización de teorías y experiencias relacionadas con la geopolítica y se adoptó una vez concluida la Segunda Guerra Mundial. Se inscribió en el marco de la Guerra Fría desarrollada desde 1945 por los grandes centros de poder militar". En este sentido, una de las características representativas fueron la institucionalidad política de las Fuerzas Armadas, y su intervención al Estado frente al poder político (Laborie, 2011). Así, para Leal (2003), la doctrina de seguridad nacional originada en los años setenta en América Latina se establece desde una visión militar del Estado, la legitimidad a la ocupación de las instituciones se otorga debido a la vinculación existente con el funcionamiento y bienestar de la sociedad. Esta percepción ubica al Estado

[5] Traducción de la autora

como un ente absolutista. La concepción de seguridad nacional, se encuentra en el ámbito institucional-territorial y Estado-Nación (López, 2016).

La aplicación de la doctrina, corresponde a un período en el plano regional con afectación en la mayoría de países en Latinoamérica. El cambio de la dinámica de la doctrina a las actuales lógicas de seguridad tiene origen en los inicios de los años setenta y la declinación de la doctrina comienza con el proceso de redemocratización, así, menciona Leal (2003):

> (...) por primera vez en más de un siglo, las dictaduras en el continente son casi inexistentes. No hay apoyo internacional al modelo militar, no hay soporte externo a los movimientos subversivos y las instituciones castrenses se encuentran en una especie de "crisis existencial". (Leal, 2003, p.2)

Sin embargo, con el fin de Guerra Fría la doctrina se quedaba sin fundamento político y las consecuencias de las finalizadas dictaduras resaltaban la violación y el irrespeto de los derechos humanos. En efecto, los diferentes países replantean la dirección de las instituciones, y empiezan a integrarse dentro de las dinámicas de la globalización con la inclusión de nuevos actores.

En cuanto a la ampliación del concepto y el cambio de agendas, con el fin de la Guerra Fría, la integración a la globalización y los hechos ya puntualizados; el sistema internacional necesita cambiar el enfoque a los problemas que hacían frente los países. Desde el punto de vista teórico, se han desarrollado diversas líneas conceptuales de la seguridad. Desde una visión de las teorías críticas y el constructivismo, los intereses de la nación se originan en las bases sociales, es decir, se construye la identidad que se refleja en los actores internacionales. Para el constructivismo, el objeto referente de seguridad es la identidad de los grupos, colectivos e instituciones que influyan en el sistema. Ahora bien, Buzan (1998) amplía el concepto de seguridad incluyendo sectores como el social, ambiental, económico, con la adaptación de actores diferentes al Estado y analizando la interacción que se origina entre ellos (Orozco, 2006). Igualmente, Alexander Wendt (1992) establece que las normas e instituciones se derivan de un proceso de construcción sobre la base de las identidades e intereses (Nobile, 2003).

En este contexto, en 1994, la Organización de las Naciones Unidas (ONU), y en específico su Programa de Desarrollo (PNUD) incluye en un informe anual que analiza el desarrollo humano y se deriva en el concepto de seguridad humana[6] que se considera como una alternativa a los problemas que no se pueden resolver con el concepto tradicional de seguridad nacional como se destaca en el informe: "la búsqueda de seguridad humana debe efectuarse a través del desarrollo y no mediante las armas" (PNUD, 1994, p. 1). Esta descripción surge debido a que se comienza a tomar en cuenta otros elementos que amenazan al ser humano y los intereses nacionales, derivados de factores políticos, económicos, sociales y medioambientales (Berea, 2009). Para Jorge Nef, (2002) la seguridad humana es la disminución del riesgo desde la esfera de la colectividad, enfocada más allá de las "expresiones sintomáticas", pues su importancia recae en el análisis de las causas y los contextos en los que se forja la inseguridad. El concepto engloba la seguridad de la persona y de la comunidad e, incluye la protección y potenciación de la persona bajo la visión de los derechos humanos (Rojas & Álvarez, 2012). En este sentido, los Estados deben hacer frente a los riesgos tomando en consideración varios factores y frentes, proyección que amplía el rango de los países para impulsar sus agendas en la creación de instituciones, políticas y leyes.

Ante lo expuesto, la crítica recae en la falta de concreción y aplicación del concepto de la seguridad humana. Para Francisco Rojas y Andrea Álvarez (2012) al ser un concepto holístico toda amenaza puede encontrarse bajo el ámbito de influencia y, al abarcar diferentes temáticas no se puede incidir efectivamente en todas. El enfoque de seguridad humana y el desarrollo del concepto desde la apreciación de Karlos Pérez de Armiño (2006) y Edward Newman (2010) carecen de sentido crítico, y a un nivel práctico no se encuentra lo suficientemente sólido para plasmar en las políticas públicas. Para Newman (2010), la aproximación teórica a la seguridad humana ha tenido diversos análisis enfocados en las consecuencias suscitadas y no en la estructura en sí de las instituciones (Larenas, 2013).

[6] El concepto de seguridad humana tiene sus antecedentes en la Declaración Universal de Derechos Humanos en 1948, pero una vez presentado el Informe sobre el Desarrollo Humano en 1994 por el PNUD se introduce formalmente el concepto y toma notoriedad dentro de la agenda internacional (PNUD, 2011).

Con el análisis anterior, y de acuerdo a la secuencia de hechos que se han suscitado, sin dejar de lado que la construcción del concepto se desarrolla de manera continua, surge un nuevo escenario internacional basado en las percepciones de las amenazas que se expanden por la globalización y la mayor interdependencia de los diversos actores, que ha permitido que el planteamiento tradicional de seguridad en términos militares surja y, por otro lado, se amplíe el concepto dentro de la agenda de seguridad para concretar respuestas enfocadas en la aparición de nuevas amenazas entre las que se pueden destacar las relacionadas a la ciberseguridad y ciberdefensa[7].

1.1.3. La ampliación de la seguridad desde un enfoque integral

El concepto de seguridad integral es planteado para ir más allá de la discusión sobre la seguridad humana y enfatizar la necesidad de mantener coherencia entre todas las políticas para promover y proteger el desarrollo humano. La seguridad integral se aproxima a equilibrar dimensiones políticas, económicas, socio-culturales y ambientales y, responde a la inclusión de nuevos factores (Laborie, 2011). Como concepto se encuentra en proceso de construcción y considera de manera secundaria los cánones tradicionales (Sánchez, 2015).

La seguridad integral desde Ballesteros, se desarrolla en lo político-militar, económico y ambiental, y humana (Sánchez, 2015, p.56). En la primera dimensión, se presenta un enfoque amplio que se centra en el ámbito militar, desde los principios de apertura, transparencia y cooperación. En cuanto a lo económico, la seguridad integral se orienta a la promoción de la cooperación económica a través del buen manejo de la gestión pública, en relación al medio ambiente, se considera un elemento fundamental puesto que aborda los recursos naturales desde la distribución y cooperación. Finalmente, la dimensión humana, propone que el mantenimiento de la seguridad integral, se consigue mediante el respeto de los derechos humanos y el bienestar, pues el Estado de Derecho tiene como objetivo preservar la vida y la integridad humana (Sánchez, 2015).

[7] El tema de la ciberseguridad y ciberdefensa serán tratados en la siguiente sección.

Siguiendo a Camilo Zambrano y Daniel Gudiño (2013) desde una visión latinoamericana, en el campo de la seguridad las amenazas transnacionales, las afectaciones por desastres naturales, el consumismo y las "nuevas amenazas" como el ciberataque, representan un desafío político para los Estados latinoamericanos que todavía se encuentran en proceso de profundización del Estado de derecho, y la responsabilidad de proteger sus ciudadanos dentro y fuera del Estado. La seguridad integral o llamada también seguridad pública y de Estado para los autores "implica la securitización de amenazas no tradicionales, es decir, la posibilidad de prevenir y mitigar los riesgos que pueden desestabilizar las sociedades y Estados, sin diferenciar el origen (en un sentido territorio) o sin la necesidad, en sí misma, de que existan ataques armados" (Camilo Zambrano y Daniel Gudiño, 2013, p.64).

La seguridad integral en cierto sentido, responde a la visión de la seguridad multidimensional derivado de los elementos que conforma y se acopla a la realidad de los países, sin embargo, se vincula en la focalización del individuo y la sociedad, sin dejar de lado los conflictos tradicionales provenientes de los Estados. En esta línea argumentativa, existen elementos que se fundamentan en la seguridad humana, no obstante, la seguridad integral no ha sido explorada plenamente en el ámbito académico y se ha utilizado como un instrumento discursivo que se acerca a las diversas temáticas de seguridad con tintes constructivistas.

Así, en el escenario propuesto el Estado sigue siendo la principal organización política y actor en el panorama internacional encargado de responder a las demandas de la ciudadanía con el objetivo de preservar el bien común. En adición, la seguridad continúa formando parte fundamental para el desarrollo y el bienestar de los países. Es así, que se puede establecer que la seguridad está ligada a los instrumentos a disposición del Estado, además, de la arquitectura, instituciones, políticas, leyes y funciones. El Estado tiene diferentes instrumentos a su disposición como: políticos, económicos, diplomáticos, militar, judicial, policial y cultural. (Griffiths, 2007).

1.2. La relación entre el Estado, la tecnología y la seguridad

La adopción e implementación de la tecnología en la seguridad han modificado las instituciones relacionados con la seguridad nacional, y se han estructurado en torno a la gobernanza y soberanía de las redes. Es por ello que, Castells (1996) sostiene que la tecnología con la intervención del Estado, se puede desarrollar y alcanzar la modernización tecnológica adecuada que influya en la economía, el dominio militar y el bienestar de la sociedad. En efecto, el potencial tecnológico de cada sociedad es decisivo en cada periodo histórico, además, la relación existente entre tecnología y sociedad está determinada por el rol del Estado y sus instituciones, considerando que organiza las fuerzas sociales y culturales en un establecido espacio y tiempo (Castell, 1996).

Entonces, se puede destacar la evolución de un nuevo dominio virtual y las dinámicas que desarrollan sus actores. En esta línea de pensamiento, se presentan dos temas centrales que se conocen como el "ciberespacio" y un concepto derivado desde la perspectiva militar la "ciberdefensa". Los enfoques demuestran en primera instancia un análisis de los términos y en una segunda, las relaciones entre los elementos e instrumentos que los actores utilizan en este nuevo escenario.

1.2.1. Nuevo dominio y nuevas amenazas: el ciberespacio

El ciberespacio es el resultado de la ciencia y tecnología, es un concepto abstracto debido a que se trata de un dominio no físico[8] y ahí la dificultad de definirlo. En efecto, la observación que Strate (1999:383) hace al ciberespacio desde una visión general, entendiendo que, al estar en todas partes y de uso creciente, su significado se ha vuelto impreciso y agotado. No obstante, si se analiza desde su ubicuidad, el concepto se limita a la multiplicidad de complejidades que presenta (Zhang & Jacob, 2012). Para comenzar, según Joseph S. Nye (2010) el término "ciber" es un prefijo para las actividades electrónicas y

[8] Dominio creado por sistemas informáticos, dónde las personas y organizaciones utilizan las Tecnologías de la información y la Comunicación (TIC) para interactuar en este espacio. El ciberespacio es medio sintético, dominio de realidad virtual forjado a finales del S. XX. (Llongueras, 2011).

relacionadas con la informática. Esta puntualización tiene como objetivo señalar que este prefijo se utiliza en varios términos relacionados y derivados del ciberespacio a lo largo de la sección.

El término ciberespacio desde un acercamiento histórico y mencionando sus orígenes, se puede entender en la obra de William Gibson titulada Neruromante (1984) en donde es un concepto ligado a la ciencia ficción y lo describe como "una alucinación consensual" donde se encuentra en el *modus vivendi* de legítimos operadores, el autor describe como "la representación gráfica de la información abstraída de los ordenadores del sistema humano" (Gibson, 1989, p.35). Desde esta aproximación, se inicia la comprensión de la realidad articulada a la tecnología y el mundo virtual desde una perspectiva visionaria (Joyanes, 2010). Para Ottis y Lorents (2010) esta definición expone el potencial desarrollo de la experiencia en el ciberespacio. A partir desde esta propuesta inicial, en el manifiesto de John Perry Barlow (1996) titulada "Declaración de Independencia del Ciberespacio" establece que el "ciberespacio consiste en transacciones, relaciones y el pensamiento en sí mismo, que se extiende como una ola en la red de nuestras comunicaciones"[9], además, Perry Barlow (1996) describe el ciberespacio como "el nuevo hogar de la mente". Desde esta conceptualización, el término extiende su espacio del físico y del tradicionalmente geográfico, conjuntamente, resalta temas como la soberanía independiente de los Estados sobre este nuevo dominio.

Por su dimensión, el concepto del ciberespacio según Daniel Kuehl (2014) es:

> Un dominio global dentro del entorno de la información cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando tecnologías de la información y la comunicación[10]. (Kuehl, 2014, p.4)

[9] Traducción de la autora
[10] Traducción de la autora

Para comprender los elementos principales del ciberespacio Nicholas Tsagourias (2015) explica que existen tres niveles: el físico que consiste en dispositivos, componentes y la infraestructura; el segundo que constituye la distribución de software[11] y; el tercero que se compone de paquetes de datos y electrónica. En este razonamiento, el núcleo del ciberespacio es el dominio virtual, comprendido por objetos físicos que establecen la conectividad con el mundo físico, y la interacción en el ciberespacio es realizado a través de logística en lugar de actos físicos, de este modo, el ciberespacio es independiente de las variables de tiempo y el espacio (Tsagourias, 2015). Una observación adicional de los tres niveles mencionados, es el efecto que resulta de la cognición humana y sus organizaciones, es decir, el acceso de los contenidos afecta el comportamiento humano y la toma decisiones (Kuehl, 2014).

En este marco, después de aportar con el análisis conceptual del ciberespacio y sus elementos, es de particular importancia para el desarrollo de la investigación un enfoque desde el acercamiento de la seguridad estatal al concepto. Al respecto, Adrianna Llongueras (2011) establece que:

> El ciberespacio es un elemento de poder dentro de la seguridad nacional, a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias forjándose y desarrollándose el concepto de "operaciones militares centrada en redes". (Longueras, 2011, p.19)

Dicho análisis, sitúa al ciberespacio como un elemento en consideración de las actividades militares. Lo anterior ha permitido que los límites territoriales y el dominio militar se extendieran en tiempo y espacio y surjan nuevas amenazas. La diferenciación que las caracteriza es que no tienen un remitente claro, además, ya no son provenientes específicamente de los Estados. El resultado de las amenazas cibernéticas se relaciona en conjunto con el desarrollo y la accesibilidad tecnológica (Theiler, 2011).

[11] El software es el elemento lógico de los dispositivos, es decir, los programas, sistemas de información y operativos y aplicaciones (Vélez, 2013).

Desde la óptica de la seguridad, en el ciberespacio existen multiplicidad de actores que se clasifican en la categoría de atacantes, que incrementan los riegos y amenazas de distintos servicios de la administración pública, por tal motivo las acciones en cuanto a seguridad estatal en este espacio son temas que predominan (Centro de Estudios para la Defensa Nacional, 2015). En esta línea de pensamiento, las dinámicas a través del ciberespacio pueden ser utilizadas como fuente de poder, las implicaciones de actividades políticas, sociales, económicas y militares dependen de este espacio y, por lo tanto, son vulnerables de la interrupción como de la usurpación de sus capacidades. Con este panorama, los aspectos del ciberespacio no se diferencian de otros dominios en cuanto las fuentes de poder y como se emplean en el espectro del conflicto (Kuehl, 2014). Es ante esta perspectiva, que en la subsección siguiente se analiza el ciberespacio desde la militarización.

1.2.2. La militarización del ciberespacio: la ciberdefensa

Las diferentes definiciones que se derivan del ciberespacio como es la ciberdefensa y ciberseguridad son parte de la variedad de términos que se utilizan sobre las implicaciones militares; sin embargo, no existe un consenso teórico o acuerdos jurídicos y, se encuentran en un constante debate. De este modo, la dispersión terminológica ha limitado la atribución de responsabilidad y la toma de decisiones a nivel político y militar (Eissa, Gastaldi, Poczynok, & Tullio, 2012). Con este panorama, el análisis terminológico es un elemento presente dentro de la investigación y el desarrollo de esta subsección.

Las nuevas y complejas amenazas en el dominio del ciberespacio han originado que se pongan en riesgo diversas áreas de los Estados, por tal motivo las acciones y el actuar eficaz y eficiente de la seguridad estatal sitúa estos temas en el ámbito militar (Valencia, 2014). Los conflictos en el ciberespacio se presentan como conflictos asimétricos y de manera anónima y, evolucionan siguiendo el progreso de las Tecnologías de la Información y la Comunicación (TIC) (Anca, 2015). Desde esta reflexión, parece lógico que en la Cumbre de la OTAN en Lisboa (2010) el general estadounidense Keith Alexander quien fue director de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) y

Comandante del Cibercomando de Estados Unidos (USCYBERCOM, por sus siglas en inglés) planteó la necesidad de militarizar el ciberespacio con el objetivo de proteger el derecho a la privacidad de los americanos (Joyanes, 2010).

A partir desde el enfoque de militarización, diversos razonamientos se han sostenido, sobre esta situación Ganuza (2010) explica que la militarización de la red:

> (…) no debe ser entendida como una ocupación de la red por fuerzas militares con el objetivo de controlar los movimientos en ella, sino como el derecho de las naciones a disponer de ciber armamento en defensa de sus legítimos intereses. Nuestros enemigos las poseen y las usan. Una percepción mal entendida que confine la capacidad militar a los medios convencionales nos pondría en una clara y peligrosa situación de desventaja. (Ganuza, 2010, p.169)

Al respecto, el ciberespacio para Néstor Ganuza (2010) debe ser considerado y analizado por su potencial inclusión en la doctrina militar para combatir y defender este espacio. Por su parte Saint Pierre (2004) expone que en la mayoría de las ocasiones se recurre al factor militar en temas que podrían aproximarse con políticas públicas. Estas cuestiones, reflejan lo contemporáneo del término y su empleo, específicamente en cómo se deben gestionar las operaciones cibernéticas frente a las amenazas de la seguridad sobre las estructuras de los Estados. Es ante esta disyuntiva, que diferentes Estados se han centrado en la intervención militar debido a las implicaciones que resultan del ciberespacio, igualmente, el entorno de la defensa resulta de interés, puesto que las operaciones virtuales tienen la capacidad de ocasionar alteraciones y modificaciones en el espacio físico (Eissa, Gastaldi, Poczynok, & Tullio, 2012).

Partiendo de lo expuesto, la militarización del ciberespacio responde tanto a la incertidumbre como al análisis estratégico de las naciones. En el ámbito de la defensa, las TIC que una vez fueron usadas para aumentar la capacidad operacional de las fuerzas armadas, en este panorama, son necesarias para proteger y combatir en el ciberespacio. Esta transformación modificó los

conceptos y doctrinas con el objetivo de adaptar este nuevo dominio. Fue de esta forma que en varios países se comenzó a analizar y estructurar la agenda de la ciberdefensa (Centro de Estudios para la Defensa Nacional, 2015).

En este entorno complejo, la ciberdefensa se puede definir en concordancia con Cano (2013) como:

> Una nueva connotación sistémica y sistemática que deben desarrollar los gobiernos para comprender ahora sus responsabilidades de Estado, en el contexto ciudadano y de fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la compresión de variables, entre otras, las vulnerabilidades en la infraestructura crítica de una nación, las garantías y los derechos de los ciudadanos en el mundo en línea, la renovación de la administración de justicia en el entorno digital y la evolución de la inseguridad de la información en el contexto tecnológico y operacional. (Cano, 2013, p.115)

De la definición planteada, se propone un nuevo modelo en el que el Estado es el eje central de un escenario atemporal y de actores mutables. En este sentido, requiere una renovación de diversas áreas, que demandan recursos y tiempo. Considerando lo anterior, Enrique Stel (2014) establece que el primer obstáculo es la concepción cultural de los responsables sobre las circunstancias del desarrollo del ciberespacio, la ciberdefensa y la ciberseguridad.

En el análisis de la conceptualización de la ciberdefensa se destaca otro término complementario, la ciberseguridad. Este concepto se define como "la organización y recopilación de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados para el ciberespacio de ocurrencias que desalinean de jure y de facto los derechos de propiedad"[12] (Craigen, Diakun-Thibault & Purse, 2014, p.16). En la misma línea de pensamiento, siguiendo a Pablo Camps (2016) la ciberdefensa debe ser entendida como las actividades reactivas frente a una amenaza.

[12] Traducción de la autora

Considerando lo anterior, el ciberespacio promueve que los Estados revisen las estrategias y agendas de seguridad en el contexto de confrontación y defensa de la gobernabilidad (Cano, 2010). Así mismo, requiere ser analizado en un contexto nacional, en donde se debe establecer si es necesaria la militarización o se puede solventar con políticas públicas que permitan respaldar la soberanía de cada Estado.

1.2.3. El nuevo campo de batalla: actores y operaciones cibernéticas

Al analizar el rol de la ciberdefensa desde el ámbito de la seguridad estatal se presentan y se identifican diversas interrogantes sobre quién o qué y, cómo se categorizan los diversos actores. Por otra parte, considerando que el ciberespacio es un dominio operacional, es necesario establecer cómo se desarrollan las dinámicas de los sujetos dentro de este espacio. En efecto, el ciberespacio se ha convertido en un nuevo campo de batalla que abarca las acciones derivadas del conflicto y que se extienden a este escenario. Por tal razón, el análisis a lo largo de esta subsección tiene como objetivo establecer las operaciones cibernéticas dirigidas específicamente a los Estados y sus estructuras.

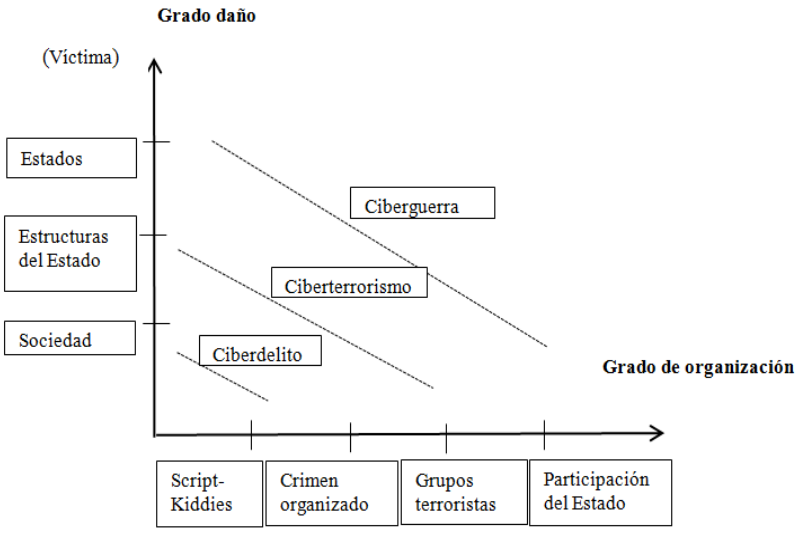
La operatividad ha primado en el desarrollo del ciberespacio y continuamente se han detectado vulnerabilidades en la seguridad, así Javier López de Turiso (2012, p.133) menciona vulnerabilidades "físicas y lógicas, en sistemas operativos, también en aplicaciones y protocolos de comunicaciones". En este escenario, se puede amenazar o atacar los tres niveles del ciberespacio ya expuestos en la subsección 1.2.1. De este modo, se han beneficiado diferentes sectores y grupos, surgiendo el ciberdelito, el ciberterrorismo y la ciberguerra.

En cuanto a las motivaciones, se pueden mencionar intelectuales, económicas, políticas e ideológicas en las diferentes categorías de ataques. En términos de ciberdelito y sin profundizar en el tema debido a la delimitación de analizar operaciones cibernéticas que afectan a la defensa nacional y, considerando que comúnmente estos ataques son abordados por las instituciones de seguridad pública (Eissa, Gastaldi, Poczynok, & Tullio, 2012), se puede encontrar que las motivaciones van dirigidas principalmente al beneficio

económico de manera ilegal. En efecto, se pueden ejemplarizar actividades como el robo de identidad, fraudes financieros, robo de datos, sabotajes y varios ataques como la extorsión (Díaz, 2010).

Por otra parte, el ciberterrorismo, según Mark Pollit (1998) establece que es el ataque planificado con causalidad política, dirigido a la información, datos y sistemas, además, el autor menciona que "pueden resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos". De acuerdo a esta afirmación, el ciberterrorismo puede llegar a vulnerar las estructuras del Estado. En cuanto a la ciberguerra, es esencial mencionar que el concepto se encuentra influenciado por clásicas estrategias y doctrinas de inteligencia (Eissa, Gastaldi, Poczynok, & Tullio, 2012). Por último, la ciberguerra corresponde a la categoría militar puesto que el alcance del ataque se desarrolla en un contexto bélico y consiste en interrumpir o destruir datos, información y los sistemas de comunicación (Eissa, Gastaldi, Poczynok & Tullio 2012). Otra aproximación presentada por Erik Gartzke (2013) mantiene que la ciberguerra todavía es una dimensión en evolución y es una fuente de preocupación, sin embargo, en términos estratégicos de mayor nivel todavía permanece en una categorización estratégica baja.

GRÁFICO 1
ATAQUES CIBERNÉTICOS



Fuente: La Ciberseguridad en el Ámbito Militar, 2010
Elaborado por: Cristina Salinas

En el gráfico propuesto, se utiliza un diagrama con el objetivo de diferenciar los límites entre los conceptos de ciberdelito, ciberterrorismo y ciberguerra. Así, se puede establecer una relación entre el grado de daño y el grado de organización del atacante (Díaz, 2010). Al analizar el gráfico se observa la progresión de ataques a la sociedad, a estructuras estatales (instituciones) y, finalmente a los Estados que es la etapa previa a la ciberguerra. En el mismo sentido, los actores comprenden desde los script-kiddies[13], el crimen organizado, grupos terroristas y la participación del Estado. Mientras aumenta el nivel de organización y técnicas operacionales, el grado del daño y alcance es mayor. En este punto, es importante establecer que los ataques evolucionan constantemente en conjunto con la tecnología y, por lo tanto, en el impacto que generan.

Adicionalmente, uno de los temas que se destaca y se encuentra como una herramienta dentro de los ataques ya mencionados es el ciberespionaje, que de acuerdo con Juan Díaz (2010) se reconoce como una extensión del espionaje clásico, con el objetivo de adquirir información confidencial de Estados o de sus instituciones críticas como las de seguridad y que brindan ventajas competitivas y superioridad estratégica frente a los otros Estados.

Finalmente, en este nuevo escenario, existe asimetría en relación al poder de los diversos actores, sin embargo, el poder del Estado se reduce respecto a éstos, además, comienza la intervención de actores no estatales en un reequilibro de fuerza, que supone un reto el monopolio del uso de la fuerza por parte de los Estados (Gómez, 2012). Esta situación también para Joseph S. Nye (2010, p.4) afirma "la dependencia de sistemas cibernéticos complejos para apoyar las actividades militares y económicas crea nuevas vulnerabilidades en los grandes Estados que pueden ser explotadas por actores no estatales".

[13] El término script-kiddies se define como el grupo de h*ackers* que utilizan técnicas, programas o scripts ya existentes, conocidos y fáciles de encontrar, con el objetivo de buscar y aprovechar las debilidades de otras computadoras (Mead, Hough, & Stehney, 2005).

1.3. El Estado desde un acercamiento al internet

El ciberespacio se ha convertido en un dominio disputado y el internet se ha centrado en ser un medio esencial de comunicación y organización. El internet se ha desarrollado como un soporte tecnológico del ciberespacio. Al ser un instrumento tecnológico al analizarlo por sí solo, se centraría la investigación en el aspecto técnico, no obstante, las implicaciones sociales que se han suscitado han cambiado el rol de los diferentes sujetos (Merejo, 2007). De este modo, los Estados y sus instituciones han centrado sus recursos en insertarse al internet y a las dinámicas del ciberespacio, pues el internet es considerado como una plataforma a este nuevo dominio.

El ciberespacio y el internet se han convertido en objeto de estudio transversal en las relaciones provenientes de los países. Así, se realiza la distinción entre internet y ciberespacio. Además, se analiza la interacción que se suscita entre el internet y el Estado, centrándose en áreas como la gobernanza, la participación del Estado, el proceso de tomas de decisiones vinculadas a la ciberdefensa y el tema de la seguridad y privacidad.

1.3.1. La inserción del Estado en el debate: el rol de internet

El debate en la centralidad de la ciencia y la tecnología es un tema que se encuentra en la opinión pública, debido a su constante transformación y sus efectos dentro de la sociedad. De esta forma, el Estado se ha integrado en la discusión y en la organización de los recursos en relación a estos temas, en especial en los vinculados con el ciberespacio. Además, de aproximarse el Estado a la ciberdefensa mediante sus instituciones y militarización, se ha preocupado por el tema del internet sus políticas, leyes y su extraterritorialidad.

Efectivamente, el ciberespacio forma parte de la soberanía estatal y está vinculado al Estado debido al flujo de información transnacional que se lleva a cabo y por la estructura de este dominio. De acuerdo con Diego Llumá (2014), la conformación en la soberanía del ciberespacio podría categorizarse como "interdependencia" puesto que se controla diversos aspectos como el flujo de

personas, materiales e ideas a través de dominios territoriales con el uso de las TIC. Así, los Estados se encuentran limitados en su competencia territorial y a la vez dependen de otros actores, mientras que el internet atraviesa las fronteras. Por tal razón, al Estado le resulta complejo adaptarse a la evolución y a la velocidad de la tecnología.

Ciertamente, al analizar el término del ciberespacio se hace visible en los hallazgos que dentro de su sistema de organización y distribución se encuentra el Internet. El internet es un factor decisivo en la planificación estatal, es la red global informática que opera mediante plataformas inalámbricas y dispositivos, y proporciona interactividad sin limitarse al tiempo y ni al espacio (Castells, 2014). El internet forma parte central del ciberespacio, y es conocido como una de sus manifestaciones más reconocidas, sin embargo, el ciberespacio comprende incluso las interacciones de dispositivos y sistemas no conectados a internet (Álvarez & Vera, 2017).

En términos etimológicos, el internet se deriva de dos palabras en inglés *inter* y *net*, traducidas al español la primera significa entre y la segunda redes (Merejo, 2007). El internet se origina siguiendo a Andrés Merejo (2007) como parte de la evolución histórico-tecnológica y tiene su propia geografía, la cual se conforma de redes y procesan flujos de información. Para entender el funcionamiento en términos estructurales se distinguen dos características y principios de internet, de acuerdo a Paz Peña (2013): en primer lugar, la red no es centralizada, es decir, no existe un nodo central que controle completamente los contenidos en internet. No obstante, la concentración de recursos críticos[14] en un conjunto de países demuestra la vulnerabilidad de distintas conexiones. Segundo, la red es neutral, así, no existe distinción de cualquier máquina conectada en relación a los paquetes de datos y origen.

En la práctica el internet tiene varias áreas privadas y públicas de gobernanza. Es así, que el internet implica diversas relaciones entre organismos,

[14] Los recursos críticos de internet son componentes indispensables para su funcionamiento, entre los que se puede mencionar las direcciones de protocolo de internet (IP, por sus siglas en inglés), el Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) y los Sistemas Autónomos (Cortés, 2014).

Estados e intereses que definirán su rol. Los gobiernos tienen un papel fundamental no solo en mantener satisfecho el amplio espectro de necesidades públicas, sino también de políticas, leyes y avances en investigación y desarrollo tecnológico que impulsen el conocimiento. Además, se debe agregar el tema de resolver problemas que resultan de decisiones independientes de los diferentes países (Kahn, 1995).

Este entorno complejo requiere que las políticas públicas estén alineadas en relación a la ciberdefensa, el ámbito militar se encuentra enfocado en reducir las vulnerabilidades y las instituciones tienen que desarrollar una metodología que enfrente las diversas amenazas en una red de convergencia. El internet al ser una de las expresiones más evidentes promueve términos como la gobernanza de internet, donde se plantea decisiones en base a la ciberdefensa y ciberseguridad.

1.3.2. La gobernanza de internet

La gobernanza de internet se ha caracterizado por ser analizada desde distintas aristas, esto ha tenido como resultado que las diferentes perspectivas del significado impulsen diversas políticas, toma de decisiones y genere distintas expectativas. Como se pudo establecer en secciones anteriores el ciberespacio no responde a las estructuras tradicionales. Es así, que de acuerdo a Jorge Pérez (2008, p. 24) "la gobernanza de internet se emplea para referirse a la situación en que las decisiones políticas han pasado del monopolio decisorio del Estado a un producto de interacción y dependencias mutuas entre instituciones políticas y sociales, públicas y privadas".

En este contexto, la gobernanza de internet parte en un principio de un modelo multiparte que comprende la sociedad civil, la comunidad técnica, la academia, el sector privado y los gobiernos con el objetivo de garantizar la seguridad y apertura del internet a la comunidad (Pérez, 2015). Así, se propone una definición, como resultado de la Cumbre Mundial de la Sociedad de la Información (CMSI), el Grupo de Trabajo (2005) establece que la gobernanza de internet es

> el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y la utilización de Internet. (p.4)

Partiendo de esta definición, se presenta una visión descentralizada y se resalta la importancia de colaboración, interacción y organización entre los distintos actores. Por otro lado, en el área estructural y siguiendo a Yochai Benkler existen tres capas en la gobernanza del internet. En primer lugar, se establece la capa de infraestructura física del internet, que pertenece a instituciones públicas y privadas con autonomía en la administración. En segunda instancia, se encuentra la red del internet, que pertenece a la capa de "código" o "lógica" que controla la infraestructura. En términos técnicos, el software que se encuentra estructurado para conformar una sola red. Finalmente, se presenta la capa de contenidos, que comprende la información, en esta última capa, el debate recae sobre temas como: la seguridad, la privacidad, la propiedad intelectual, la libertad de expresión, la accesibilidad, etc. (Erazo, 2011).

Desde diversas perspectivas, se intenta delimitar y construir los entornos que conforman la gobernanza de internet. Así, la configuración de la gobernanza del internet desde el juicio analítico de Howard Rheingold puede resultar en lo que titula "telaraña panóptica". A partir de este razonamiento, surgen varios temas como la invasión de derechos de la privacidad y protección de datos personales por parte de entes privados y gubernamentales (Betancourt, 2012).

Para Erick Iriarte (2006), una de las problemáticas que se derivan de la gobernanza del internet es el contexto técnico que tiene incidencias sociales, puesto que contiene diversos temas que deben ser abordados en las políticas de Estado, como el escenario técnico, las regulaciones y la generación de capacidades. Además, recalca la importancia de considerar el tema transfronterizo que exige una visión global, en conjunto con el análisis de las características de cada Estado y con la incorporación de las TIC. Igualmente, los inconvenientes de acuerdo a este autor comienzan cuando la gestión y funcionamiento no se

encuentran en la soberanía de cada país y el marco normativo, no cubre o aplica las diversas problemáticas.

En el panorama internacional existe divergencia de opiniones en cuanto al nivel de intervención gubernamental en las distintas capas ya mencionadas y propuestas por Yochai Benkler. En este caso, el debate incurre en temas que afectan asuntos propios de la administración pública. Además, la preocupación se encuentra en las delimitaciones de autonomía y en la participación de los actores, específicamente los que quiere formar parte de la toma de decisiones (Iriarte, 2006).

En fin, la gobernanza del internet engloba varios temas que se encuentran en debate y, en cuanto a la gobernanza todavía es necesario establecer limitaciones sobre soberanía, autonomía y aspectos técnicos. Ante esta nueva situación, es preciso contextualizar la problemática de la gobernanza de internet y dimensionar la responsabilidad de cada actor en base al diálogo y consenso, en especial en las cuestiones que derivan en la construcción de políticas públicas y leyes.

1.3.3. El dilema inevitable: entre la seguridad, la defensa y la privacidad

La seguridad y la privacidad en el ciberespacio parten del debate sobre el rol que debe ejercer el gobierno mediante sus instituciones y regulaciones. Por una parte, las fuerzas encargadas de la seguridad intervienen en diferentes ámbitos de la sociedad y las regulaciones limitan diferentes aspectos. Por otra parte, la sociedad civil sostiene que las comunidades en el ciberespacio pueden ser autogobernadas con poca interferencia del Estado. En efecto, la gobernanza del internet, la ciberseguridad y la ciberdefensa crean una estructura que de manera relativa y variable afectan los derechos ciudadanos por sobre el bien común. La superposición en diversos ámbitos de la privacidad y la seguridad dependen del desarrollo de políticas y leyes de los Estados (Lewis, 2012).

En la sección anterior ya se han identificado las operaciones cibernéticas que afectan la seguridad de los Estados, ante esta disyuntiva y para garantizar la ciberseguridad y ciberdefensa se han planteado alternativas para enfrentar las

amenazas. Así, el Estado tiene la opción de controlar el ciberespacio mediante el monitoreo de las acciones de los individuos. No obstante, este tema ya se ha analizado en ámbitos diferentes al ciberespacio y se lo conoce como un tema debatible en cuanto a las regulaciones del Estado que interfieren y repercuten en la libertad y la privacidad individual (Koch, 2015).

En la literatura ya se menciona la intención de control de los gobiernos e instituciones sobre el ciberespacio. Siguiendo a John Perry Barlow (1996) en la "Declaración de Independencia del Ciberespacio" ya propone el ciberespacio como un dominio independiente de intervenciones, sin embargo, se desarrolla un nuevo escenario de expansión de distintas plataformas que controlan y monitorizan a los usuarios constantemente, provocan lo que Castells menciona en base a David Lyon (2001) que "los gobiernos de todo el mundo apoyan estas tecnologías de vigilancia y se afanan en adoptarlas, para conseguir recuperar parte del poder que corrían el riesgo de perder" (García, 2015)

Desde otra perspectiva, en cuanto a la privacidad Ofelia Tejerina (2014) hace referencia al panóptico establecido por Jeremy Bentham y menciona en relación a este tema el desarrollo del "banóptico"[15] en donde el vigilado facilita la entrega de la información al vigilante y se aplica a una población en específico. Siguiendo a Sebastián Koch (2014) menciona una característica del ciberespacio conocida como "realidad dual" que se refiere a la compleja delimitación entre lo público y lo privado, es decir, la disponibilidad de información que se encuentra, este nuevo elemento se añade como un factor que dependerá de los usuarios. En cuanto a las prácticas de acceso a la información, sectores, sistemas o datos restringidos, éstos constituyen una interferencia en la privacidad y la libertad, no solo de individuos, sino de organizaciones, sector privado e instituciones estatales. Koch también menciona que esta situación aporta a que los Estados reaccionen para que la ciberdefensa y la ciberseguridad garanticen y defiendan la privacidad y la libertad.

[15] Siguiendo a Didier Bigo el "banóptico" (ban, exclusión) se aplica a grupos marginales globales. El autor explica como a través de las tecnologías elaboran perfiles que se utiliza en la vigilancia estricta (Bauman & Lyon, 2013).

Al contrario de lo expuesto, Manuel Castells en el 2001 presenta el internet dentro del ámbito de la democracia y política como elemento que fomenta el acceso a la información. En efecto, como un instrumento ideal, los ciudadanos tienen acceso a la información tanto como los gobiernos lo permitan. Desde esta visión, la información disponible puede resultar en la interactividad entre los ciudadanos y sus representantes y, la gente podría ser quien vigile a su gobierno.

Por otro lado, el rol del usuario como protagonista se extiende al concepto y reformula a lo que se conoce como Web 2.0 término propuesto por Tim O'Reilly (2004), donde el usuario gestiona la generación, intercambio y finalidad de la información y contenido y, definirá su identidad digital. En este aspecto, lo que limita al usuario es que la red como estructura no se puede controlar. Es así, que la estructura posee sistemas con controladores que permiten seguir el rastro de los internautas. De esta manera, la arquitectura del ciberespacio se forma como una amenaza a la libertad. En consecuencia, lo que persiste para los usuarios es el contenido como factor que determinará las acciones para ejercer su libertad (García, 2015).

En este marco, se adhiere el tema de la internacionalización, la extensión de las tecnologías a nivel global crea nuevas conexiones y origina un nuevo canal de comunicación. La creación de instituciones y normas no se encuentran en la jurisdicción de un solo Estado, sino de convenios que se han aproximado a varios temas relacionados con la información y la accesibilidad. Resulta importante mencionar que el ciberespacio por sus características y estructura tiene limitaciones en regular contenido. Es así, que la tensión que se funda entre la privacidad y seguridad es principalmente política, es el resultado de visiones, valores y perspectivas del futuro que se rivalizan (Lewis, 2012).

En este tema resurge y refleja la discusión existente entre privacidad y el actuar de los Estados en base a la seguridad. Es de principal importancia determinar y evaluar la factibilidad del accionar estatal; igualmente, es esencial limitar la intervención de operación en el ciberespacio sin afectar la libertad y la privacidad individual. En fin, parece que al no delimitar la vigilancia que se ha venido desarrollando, elementos del ciberespacio como el internet se encontrarían

como un espacio de falsa sensación de libertad, contrario al ideal de emancipación, democratización y libertad en los que se instituyó su creación (García, 2015).

Este capítulo ha conseguido cumplir en primera instancia, abordar el concepto de seguridad desde diferentes teorías, considerando parámetros como el objeto referente, las amenazas y los valores. En segunda instancia, aproximarse a las variaciones del término seguridad desde las perspectivas teóricas del realismo, realismo político y neorrealismo y constructivismo. Además, ha establecido las nuevas amenazas y operaciones cibernéticas que surgen a partir del ciberespacio y, la reacción de los Estados por militarizar y crear una estructura de ciberdefensa. En efecto, el internet se ha determinado como un elemento fundamental para el alcance del análisis, pues centra el debate en el resultado de las dinámicas de los diversos actores.

CAPITULO II
ESTADO DEL ARTE DE LA CIBERDEFENSA EN ECUADOR

2.1. Perspectiva histórica de la seguridad en Ecuador de 1979 a 2016

En el caso de Ecuador, la transición de un gobierno militar a continuos gobiernos democráticos contribuyó a la formación de la estructura institucional del Estado, es así que en diferentes ámbitos existe una permanencia de la influencia militar en periodos anteriores a la sucesión del gobierno correspondiente a 2007. Por lo tanto, la estructura de la seguridad y aspectos de política-estratégica respondían a una lógica militar, desde la concepción de la Doctrina de Seguridad Nacional (López, 2016). No obstante, la constante renovación de concepciones de seguridad se ha plasmado en instituciones y en el contenido de diversas políticas y leyes, de este modo el esquema de gobierno en términos de seguridad y defensa ha experimentado diferentes transformaciones través del tiempo.

Es así, que desde el 2008 mediante la nueva Constitución de la República del Ecuador se incluye una nueva concepción de seguridad, la denominada "seguridad integral"; este enfoque plantea a la seguridad como una visión multidimensional en que aspira abarcar todos los aspectos de protección del ser humano, Estado y naturaleza (Sánchez, 2015). La construcción y planificación del Estado en este contexto correspondería a una correlación conceptual con los términos planteados, de esta manera, se analiza la evolución de la seguridad y defensa desde 1979 hasta el 2016.

2.1.1. Del regreso a la democracia en 1979 al cambio de enfoque de la seguridad y defensa a partir del 11 de septiembre de 2001

Para comenzar con la explicación del proceso histórico de la seguridad y defensa, es importante establecer que existen varios momentos históricos que repercutieron en la transformación constante del Estado en temas de seguridad y defensa. Es así, que se plantea como punto de partida el retorno al sistema democrático. En Ecuador desde 1978 comienza su retorno a la democracia después del Triunvirato Militar de los años 1976-1979. Anteriormente, la agenda

de seguridad nacional no estuvo dirigida a un enemigo interno, sino a la defensa territorial y la modernización del Estado con alta influencia militar (Sánchez, 2015). Ante esta situación, la construcción social ecuatoriana y su identidad se fundan en la vinculación de la existencia del Estado en relación a la institución militar. Así, en 1979 se reforma la Ley de Seguridad Nacional que ya había experimentado modificaciones desde su primera versión en 1960 (Haro, 2010). La Ley de Seguridad Nacional promulgada en 1979 en el registro oficial N.- 887 destaca en el artículo 2 que:

> El Estado garantiza la supervivencia de la colectividad, la defensa del patrimonio nacional y la consecución y mantenimiento de los Objetivos Nacionales; y, tiene la función primordial de fortalecer la unidad nacional, asegurar la vigencia de los derechos fundamentales del hombre y promover el progreso económico, social y cultura de sus habitantes, contrarrestando los factores adversos internos y externos, por medio de previsiones y acciones políticas económicas, sociales y militares. (Ley de Seguridad Nacional, 1979, art. 2).

Desde este punto, el Estado se responsabiliza de la seguridad nacional y, cabe destacar que se comienzan a fortalecer nuevos tópicos en el concepto de seguridad relacionadas al desarrollo socioeconómico. Por otro lado, en el capítulo II se establece como autoridad máxima de seguridad nacional al Presidente de la República, a quien se concede poderes máximos ante cualquier toma de decisión, consolidando la idea de establecer límites en la responsabilidad de gobernanza. En cuanto a los organismos superiores, se presenta al Consejo de Seguridad Nacional (COSENA) y al Comando Conjunto de las Fuerzas Armadas. De acuerdo a Carlos Sánchez (2015), se comienza a crear una política institucionalizada en el ámbito de la defensa, además, se responsabiliza al Estado plantear objetivos nacionales y establece predominio a la defensa de la integridad territorial y la soberanía.

Este escenario originó como resultado que las Fuerzas Armadas (FF.AA.) expongan mediante un pronunciamiento que no se volverá a experimentar

injerencia en temas de política del país, sin embargo, el COSENA y las Fuerzas Armadas ocupan un lugar como asesores permanentes del ejecutivo y se muestran como reguladores en varias ocasiones con relación a temas de la democracia (López, 2016). Para 1981 con la presencia del conflicto bélico con Perú conocido como conflicto de Paquisha[16] resurgen y se fortalecen nuevamente ideas sobre la defensa enfocada en la soberanía, la militarización de zonas y el enfrentamiento por intereses territoriales ante la amenaza de una invasión. En esta coyuntura, las conversaciones bilaterales y la definición geográfica calmaron momentáneamente el conflicto (Torres, 2000). En secuencia con lo expuesto, en el período de 1984 a 1998[17] la seguridad y la defensa se dirigen a temas internos con la instauración de una política antisubversiva en relación a grupos subversivos de la época y predominaba la Doctrina de Seguridad Nacional, desde una perspectiva geopolítica tradicional y no se avanza en el tratamiento del conflicto externo con el Perú (Sánchez, 2015).

Con este panorama, Bertha García (2008) menciona que:

> (…) las reformas introducidas en el pacto civil-militar de la transición política en 1979, y las prácticas reintroducidas desde 1992 por los gobiernos civiles, ante la actualización del conflicto fronterizo con el Perú, tuvieron como consecuencias: a) mitigar la intervención política civil en las instituciones castrenses, b) minimizar el rol del Ejecutivo y Legislativo en los asuntos de seguridad y militares; y c) mantener en secreto el presupuesto militar. (García, 2008, p.205)

Ante este argumento, se constata la condición institucionalizada militar de los años noventa. Sin embargo, los conflictos limítrofes con el Perú se mantenían latentes, así, en 1995 se ocasionó una escalada del conflicto que desencadenó la

[16] Conflicto entre Ecuador y Perú se deriva del Protocolo de Río de Janeiro, en el que no se delimita la pertenencia territorial de las zonas ubicadas en la Cordillera del Cóndor. En el conflicto existieron acciones de baja intensidad entre el 22 de enero y el 10 de marzo del 1981 que se produjo el cese al fuego y la desmilitarización de las zonas. En la resolución de la controversia se concedió la vertiente occidental a Ecuador y la oriental a Perú (Torres, 2000).

[17] Período presidencial de León Febres Cordero

guerra del Cenepa[18], acontecimientos que finalizaron con la firma de la paz en 1998. Las operaciones militares se orientan a la defensa interna y, con la Constitución de 1998 se continúa con el enfoque tradicional y el rol de los militares quienes se encuentran responsables de los grandes temas en relación a la seguridad nacional (Sánchez, 2015). Las Fuerzas Armadas mantuvieron un planteamiento diferente en el 2000[19], pues optaron por participar abiertamente en la arena política.

Por otro lado, en el panorama internacional, los hechos suscitados el 11 de septiembre de 2001 en Estados Unidos (EE. UU) cambiaron las percepciones que hasta el momento se enmarcaban en temas de seguridad nacional, defensa, seguridad pública y ciudadana. Los nuevos escenarios instauraron relaciones civiles-militares y se instituye la cooperación internacional, la multidimensionalidad y la reestructuración de la institución militar (Benalcazar, 2008). Esta problemática, influyó directamente en los Estados para que se preparen a enfrentar nuevas amenazas como el terrorismo, el narcotráfico y el crimen organizado. Desde una aproximación regional, Ecuador se encuentra influenciado directamente, pues la seguridad y defensa se enfoca en problemas de crimen organizado en la frontera con Colombia (Sánchez, 2015).

En síntesis, la agenda de política militar se caracterizó por tres puntos fundamentales. El primer punto, se presenta como un regreso a la hegemonía de la política de seguridad de EE. UU; el segundo punto, expone las acciones militares en centrarse en los problemas vinculados al conflicto colombiano y frontera norte. El último punto, constituye el seguimiento de hechos ilegales (Ministerio Coordinador de Seguridad Interna y Externa, 2014, p.51). En definitiva, estos escenarios demuestran la relación de autonomía que mantienen los gobiernos con las Fuerzas Armadas y su intervención en asuntos públicos,

[18] La Guerra del Cenepa es el conflicto territorial entre Ecuador y Perú en la zona del río Cenepa, que se produce posterior al conflicto de Paquisha. En efecto, se caracterizó por ser un conflicto armado de baja intensidad y de alta actividad diplomática, se desarrolló desde el 26 de enero hasta el 28 de febrero. El proceso de mediación, negociación, arbitraje y acuerdo se llevó a cabo desde 1995 a 1998. El 26 de octubre de 1998 se firmó el Acta Presidencial de Brasilia, en donde se acepta por las partes la culminación del proceso (Lekanda, 2009)

[19] Cese de funciones del presidente Jamil Mahuad Witt, durante su mandato se produjo la crisis financiera de 1999 denominada “feriado bancario”.

desde el retorno de la democracia hasta 2001 se ha mantenido arraigada la Doctrina de la Seguridad Nacional.

2.1.2. Desde la elaboración de Libro Blanco de Defensa Nacional en 2002 hasta el cambio de gobierno en 2007

En continuación con los hechos y después de introducir el proceso democrático, el fin de un conflicto limítrofe, la influencia de la política de seguridad de EE. UU y el origen de nuevas controversias, definen un nuevo panorama y se incorpora la determinación de la política de defensa en el año 2002, como un proceso de restructuración de la seguridad y defensa. En el año 2002 el presidente de turno[20] expresaba "el Libro Blanco de la Defensa Nacional, aporte fundamental para la modernización del Estado, para el fortalecimiento de la confianza nacional y la vigorización del sistema democrático". En efecto, el "Libro Blanco[21] de la Defensa Nacional" se presenta como una agenda que mantiene el modelo estatocéntrico, pero incluye temas económicos, políticos, sociales y ambientales, además de la participación de actores no estatales, esta visión está relacionada con un enfoque multidimensional. También, engloba varios aspectos que no se habían mencionado antes como: extrema pobreza, antiterrorismo, escasez de recursos y migración (López, 2011).

Así, en el Libro Blanco de la Defensa Nacional (2002) se encuentran entre los objetivos de defensa la protección de la población y los recursos. Por otra parte, la política de defensa nacional se fundamenta en el "amplio consenso civil-militar" y se mantiene el carácter defensivo, donde se conserva el derecho de Estado soberano frente a la preservación de intereses nacionales. El diseño de esta política se fundamentó en el concepto de seguridad multidimensional, desertando la Doctrina de Seguridad Nacional que se había mantenido. En este sentido, se constata un importante avance en cuanto al pensamiento institucional que repercute en la defensa nacional. Para Oswaldo Jarrín (2008), dentro de esta nueva

[20] Gustavo Noboa Bejarano (2000-2003)
[21] El Libro Blanco de acuerdo con Borges y Banti (2010) es un instrumento estatal que contiene la política de seguridad y defensa, que tiene como objetivo exponer de manera transparente de al sistema internacional, en especial ante la región el manifestó la voluntad de mantener relaciones pacíficas (Sánchez, 2015).

perspectiva conceptual de seguridad se desarrolló una nueva estructura de defensa en donde se integró la academia, las organizaciones sociales e instituciones

Efectivamente, el Libro Blanco tuvo avances en la aproximación de diferentes temas, sin embargo, entre los temas que no se abordaron plenamente, se encuentra la ausencia del control institucional de los órganos de inteligencia (López, 2011). Pablo Celi, asesor del Ministerio de Defensa mencionó que el Libro Blanco:

> (…) no logró una modificación del sector de la defensa en las formas de relación política y no estuvo acompañado de una transformación institucional, ni que sus contenidos se articulen con reformas en el campo legal que permitan un nuevo posicionamiento social e institucional de la política de defensa sugerido (Jarrín, 2008).

Siguiendo a Carlos Sánchez (2015) el Libro se puede se puede sintetizar en la determinación de políticas de defensa frente al nuevo escenario geoestratégico y las nuevas amenazas que se desencadenan del nuevo orden mundial.

La constante inestabilidad en el panorama político desencadenó que se considere como prioridad la reforma del Estado y la política de defensa en relación a la situación interna y externa del país. A partir de la destitución del Presidente[22] correspondiente al período 2003-2005 y la asunción al poder del siguiente gobernante[23], se estableció como objetivo realizar cambios para alcanzar un proceso de despolitización institucional del sector de la seguridad. En este sentido, se presenta la oportunidad de fortalecer y estructurar las instituciones y la agenda de defensa nacional (Jarrín, 2008). El presidente conformó la Directiva de la Defensa Nacional que, en líneas generales, se mantiene dentro del enfoque multidimensional y plantea la elaboración y ejecución de la "Agenda de Defensa Nacional 2005-2006", actualización del Libro Blanco, la articulación ministerial, la transparencia en relación a la rendición de cuentas, la participación de la

[22] Lucio Gutiérrez
[23] Alfredo Palacio (2005-2007)

ciudadanía y además, consolidar la relación civil-militar como propuesta continúa del Libro Blanco de 2002 (Montúfar, 2006).

A partir de las propuestas presentadas, la actualización del Libro Blanco (2006) se plantea con nuevos temas que se basan en el conflicto trasfronterizo de Ecuador-Colombia y las amenazas que se derivan de esta relación, como el amplio tema de desplazados y refugiados, flujo de droga y violencia organizada, igualmente, se considera la cooperación en la estabilidad de la paz regional y la reestructuración coordinada de las FF.AA. No obstante, no existe variación en cuanto los objetivos del Libro Blanco 2002. En relación a la estructuración de la "Agenda de Defensa Nacional" tuvo como objetivo reunir a diversos actores de la sociedad. La Agenda se planeó con una temporalidad de 16 meses (2005-2006) y tuvo como prioridad el tema legal, educacional y doctrinal de las FF. AA y la actualización de la Política de Defensa. Por último, el Libro Blanco de la Defensa Nacional se mantiene hasta el año 2007. En el período presentado no se consolidan los cambios propuestos, debido al constante cambio de gobiernos y el corto período de tiempo para su aplicación y el análisis de los resultados obtenidos.

2.1.3. La necesidad de una nueva visión de seguridad del 2008 hasta el 2013

Este último análisis histórico nos acerca a las concepciones delimitadas en la investigación en torno a la seguridad y defensa. En el período del presidente electo en 2007[24], entra en vigencia la nueva Constitución (2008) y las implicaciones en materia de seguridad y defensa se replantean y se direccionan a un enfoque integral (ver Anexo 1), igualmente, se reflejan como un quiebre del modelo tradicional militar. A partir de este momento, Ecuador asume la responsabilidad de delimitar la conceptualización y su aplicación en las instituciones mediante políticas y leyes. En este sentido, el Estado cumple un rol fundamental y el pleno ejercicio en los procesos de seguridad y defensa.

Tal como se mencionó anteriormente, la Constitución del 2008 consiguió diversos cambios en los ámbitos que se derivan de la seguridad. Así, entre los

[24] Rafael Correa (2007-2017)

deberes primordiales del Estado se detalla en el art 3., numeral 8 “Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción”. De esta manera, el enfoque de seguridad integral se inicia en la Constitución de la República del Ecuador (2008), se articula en el Plan Nacional del Buen Vivir (PNBV) período 2009-2013, la Ley de Seguridad Pública y del Estado (2009), y se desarrolla en el Plan Nacional de Seguridad Integral (PNSI) período 2011-2013, en donde se aplican las políticas, estrategias y acciones, es decir, es un elemento transversal.

Antes de abordar el tema es importante mencionar que el primer documento que establece la posición oficial y menciona los elementos sobre la seguridad integral es la Agenda Nacional de Seguridad Interna y Externa (2008), de esta manera, la seguridad integral en Ecuador comprende el accionar del Estado y la sociedad desde la concepción íntegra y humana, que abarca temas de gobernabilidad, democracia y derechos humanos. Además, se incluye la importancia de la integración latinoamericana, las relaciones Sur-Sur y la seguridad global.

Considerando lo planteado, la nueva visión de seguridad reconoce el escenario multidimensional en cuanto a amenazas que se encuentran en el entorno del ser humano y a nivel global, propone una transformación en diversas áreas como la democracia, la gobernabilidad e integración regional. Además, reconoce la interdisciplinariedad como elemento para conseguir la seguridad integral. Siguiendo a Paúl López (2016) la agenda agrega elementos de diagnóstico y, de manera general lineamientos y políticas dentro del ámbito de la seguridad y defensa a nivel político-administrativo.

En el marco normativo, desde la Ley de Seguridad Pública y del Estado (2009), se orienta a regular la seguridad integral y estructurar el tema organizacional (Ver Anexo 2). En el art. 1 se menciona:

> La presente ley tiene por objeto regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el

> marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado. (Ley de Seguridad Pública y del Estado, 2009, art.1)

A partir, de esta ley, los órganos estatales que se crean son el Consejo de Seguridad Pública y el Estado (COSEPE), en su función asesora y recomienda al Presidente en materia de seguridad. También, se crea el Ministerio Coordinador de Seguridad que se encargó de planificar y ejecutar el "Plan Nacional de Seguridad Integral (2011-2013)". Por otro lado, en el art. 11 se presentan los órganos ejecutores y en el literal a) se mencionan los órganos encargados de la defensa que son los Ministerios de Defensa, de Relaciones Exteriores y Fuerzas Armadas. Igualmente, en el art. 13 se presenta la Secretaría Nacional de Inteligencia encargada del Sistema Nacional de Inteligencia[25].

El Plan Nacional del Buen Vivir (2009-2013) abarca como ejes fundamentales el Estado, la naturaleza y el ser humano. Así desde la seguridad integral, se relaciona principalmente con los derechos humanos y la protección del individuo en los diferentes ámbitos en los que se encuentra y se desarrolla, orientándose a la calidad de vida y tópicos estructurales; además, se enfoca en el Estado e institucionalidad dentro de una visión soberana, y entre las políticas y lineamientos se define el fortalecimiento de las capacidades estratégicas de la seguridad integral. El diseño del plan se presenta como articulador de las políticas públicas en lo que concierne a la seguridad integral. En este punto, se publica, complementariamente el Plan Nacional del Buen Vivir (2013-2017), que cumple el rol de planificador y que establece los objetivos y directrices para el desarrollo.

[25] En la Ley de Seguridad Pública y del Estado (2009), artículo 14, numeral a) se establece que la "Inteligencia, es la actividad consistente en la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral. La información de inteligencia es sustancial para la toma de decisiones en materia de seguridad". Por otro lado, en el numeral b) se presenta "Contrainteligencia, la actividad de inteligencia que se realiza con el propósito de evitar y contrarrestar la efectividad de las operaciones de inteligencia que representan amenazas o riesgos para la seguridad ".

Regresando al "Plan Nacional de Seguridad Integral (2011-2013)" se planifica mediante ocho agendas de los Ministerios y Secretarías[26] y se establecen las nuevas directrices, políticas y leyes de seguridad y defensa. Las Agendas se conforman en: 1. Agenda Estratégica de Política Exterior; 2. Agenda Política de Defensa; 3. Agenda de Seguridad Ciudadana y Gobernabilidad; 4. Agenda de Justicia, Derechos Humanos y Cultos; 5. Agenda Política de Gestión de Riesgos; 6. Agenda Nacional de Inteligencia; 7. Agenda de Plan Ecuador y 8. Agenda de Estrategias de Seguridad Vial (Plan Nacional de Seguridad Integral, 2011).

En base a lo anterior, la entrega del Plan Nacional de Seguridad Integral (2011) continúa con la nueva conceptualización de la seguridad. Entonces, resulta pertinente destacar elementos del concepto de la seguridad integral planteada, como la protección de derechos humanos, libertad, gobernabilidad, justicia, democracia, solidaridad, prevención de protección y subsanar riesgos y amenazas (Plan Nacional de Seguridad Integral, 2011).

Como concepto no se define estrictamente, por el contrario, genera puntos de vista sobre el fondo y la forma en que pudiere ser utilizado, teniendo en cuenta las modificaciones que se suscitarían debido a la amplitud con la que puede ser aplicado, siendo esto útil para sucesos que eventualmente se produjeren en el panorama internacional. Por otro lado, interpretar el concepto "integral" deriva a reconocer la multiplicidad de actores y escenarios a partir del mismo (López, 2016). El concepto corresponde y se articula desde una visión de seguridad multidimensional y humana, uno de los desafíos que presenta es no elevar cada problema o amenaza al nivel de seguridad, es decir, direccionarse a la securitización; otro desafío, recae en valorar las amenazas prioritarias y secundarias.

Efectivamente, la publicación del Plan (2011-2013) abarca aspectos del ser humano, en los que se destaca como actor fundamental y transversal dentro del

[26] Los Ministerios y Secretarías se encuentran numerados de acuerdo a las ocho agendas presentadas: 1. Ministerio de Relaciones Exteriores, Comercio e Integración; 2. Ministerio de Defensa; 3. Ministerio del Interior; 4. Ministerio de Justicia, Derechos Humanos y Cultos; 5. Secretaría Nacional de Gestión de Riesgos; 6. Secretaría Nacional de Inteligencia; 7. Secretaría del Plan Ecuador y 8. Agencia Nacional de Tránsito.

proyecto, y además las capacidades y rol del Estado. En los ámbitos de enfoque se encuentran: Justicia y Seguridad Ciudadana, Relaciones Internacionales y Defensa, Democracia y Gobernabilidad, Justicia Social y Desarrollo Humano, Ambiente y Gestión de Riesgos y Ciencia y Tecnología. También se exploran temas desde la desmilitarización de la seguridad estatal hasta la protección de la naturaleza, estableciendo así un criterio que no solo reconozca lo militar y lo policial. Al respecto, se puede considerar que el gobierno establece sus propias amenazas específicas (López, 2016). En cuanto a la política de defensa, se reconoce que todavía persisten amenazas tradicionales que se desencadenaron después de la acción armada de Angostura (2008) [27], por lo que se propone el mejoramiento de las operatividad y condiciones de las FF.AA. y se destaca una vez más el fomento de la relación entre civiles y militares (Serrano, 2012). No obstante, el rol de la institucionalidad en la seguridad y defensa se considera como primordial y como un eje de funcionamiento.

Vista desde el plan del sistema internacional, Ecuador se aproxima a la "seguridad cooperativa" como un concepto en el que el sistema internacional responda a los riesgos y garantice la seguridad de los Estados y las relaciones existentes con los demás actores (Plan Nacional de Seguridad Integral, 2011). En relación a los períodos anteriores se avizora una concepción global, a diferencia de enfocarse en los países vecinos como Perú y Colombia y, mantener una influencia directa e indirecta de EE.UU. Además, en el Plan Nacional de Seguridad Integral (2011-2013) en las relaciones internacionales que desencadenen conflictos se distancia del uso de la fuerza, y promueve la no intervención en los Estados. De igual manera, se integra con cierto grado de compromiso a las aspiraciones de organismos regionales y como prioritaria a la Unión de Naciones Suramericanas (Unasur), teniendo en cuenta los diferentes cambios y amenazas que enfrentan los miembros. De manera que, acredita a nivel internacional el concepto de seguridad en el país (López, 2016)

[27] La acción armada de Angostura o también llamada "Operación Fénix" fue el bombardeo al campamento de las Fueras Armadas Revolucionarias de Colombia (FARC), que se encuentra en Sucumbíos en la selva de Angostura por parte de las Fuerzas Armadas de Colombia en el 2008. Como resultado, se dio la baja Luis Edgar Devia, alias "Raúl Reyes", conocido por ser el segundo en mando y 22 personas más incluido un ecuatoriano. Esta situación marcó un punto álgido en las relaciones bilaterales en cuanto a temas territoriales (Moscoso, 2014).

2.1.4. Lecciones aprendidas: actualización del Plan Nacional de Seguridad Integral desde el 2014 hasta el 2016

Cuando se proyecta la seguridad integral, se presentan incertidumbres conceptuales, es así que, se plantea la posibilidad de estar frente a un cambio constante en temas de su aplicación e implementación de elementos estructurales, institucionales, normativos y políticos. En este escenario, se incorpora la continuidad del tercer período presidencial[28] que de manera directa influye para que se mantenga una línea de pensamiento secuencial en el cual, se afirma la responsabilidad de seguir con el modelo integral en materia de seguridad. En cuanto al Plan Nacional de Seguridad Integral y las agendas que contiene, se realiza una actualización en el proyecto que se elaboran para el período 2014-2017. De este modo, el nuevo plan tiene como objetivos concretar la seguridad integral en cuanto a su definición e implementación.

Ante el panorama cambiante en la arena nacional e internacional, el Ministerio Coordinador de Seguridad frente al sistema integral de seguridad realiza un proceso de seguimiento y evaluación, y publica el Plan Nacional de Seguridad Integral (2014-2017) que comprende las nuevas agendas nacionales, enfocado en tres ejes articuladores: "prevención, previsión y atención; cultura de paz y, soberanía e integración" (Plan Nacional de Seguridad Integral, 2014, p.10). A diferencia del plan anterior, éste vincula la ampliación y operatividad del concepto seguridad integral con las instituciones que conforman el Consejo Sectorial de Seguridad[29] y, por otra parte, cabe señalar que los cinco ámbitos expuestos en esta versión son: Defensa y Relaciones Internacionales, Seguridad Ciudadana y Justicia, Gestión de Riesgos y Ambiente, Soberanía Tecnológica y Ciencia e Inteligencia Estratégica para el fortalecimiento democrático. Sin

[28] Rafael Correa (2013-2017)

[29] El Consejo Sectorial de Seguridad es el organismo de la Función Ejecutiva que contiene instituciones relacionadas con la seguridad y, aprueba políticas sectoriales e intersectoriales (Plan Nacional de Seguridad Integral, 2014)

embargo, se reducen las agendas[30] a seis. En cuanto al espectro de seguridad se amplía a tres aspectos: "estadocéntrico (Estado), antropocéntrico (el ser humano) y biocéntrico (la naturaleza)" (Plan Nacional de Seguridad Integral, 2014, p.25).

GRÁFICO 2

CONCEPCIÓN DE LA SEGURIDAD INTEGRAL

Fuente: Plan Nacional de Seguridad Integral, 2014-2017
Elaborado por: Ministerio Coordinador de la Seguridad (2014)

Sobre este enfoque, Paúl López (2016) menciona que la nueva agenda analiza y amplía el concepto de la seguridad integral, que desde la perspectiva teórica tiene como propósito justificar el concepto. También, establece los elementos en su contenido formaliza la construcción del concepto y el cambio constante de las amenazas y el escenario de seguridad y defensa. El tema institucional se presenta como prioritario para la implementación de la seguridad integral y define la operatividad entre las instituciones. Es así, que en el plan se menciona que la importancia de la ampliación del concepto, es en convertir la política estatal operativa y funcional en las entidades que forman el Consejo Sectorial de Seguridad (Plan Nacional de Seguridad Integral, 2014). En efecto, la extensión de varios temas diferencia las visiones y conceptos entre la seguridad nacional, humana e integral. Además, justifica y explica la vinculación con el Plan Nacional del Buen Vivir y establece que la concepción va más allá de la seguridad

[30] Las agendas pertenecen al Ministerio del Interior, Defensa Nacional, Justicia, Derechos Humanos y Culto, Relaciones Exteriores y Movilidad Humana, Secretaría de Gestión de Riesgos y Secretaría de Inteligencia.

humana, pues propone como eje central direccionar la política pública en la protección de la vida (biocentrismo)" (Plan Nacional de Seguridad Integral, 2014, p.24). Así también, en el Plan de Seguridad Integral (2014-2017) se establecen dos grandes dimensiones: la ciudadanía y el Estado en el entorno territorial e institucional, que guía las políticas y acciones.

En resumen, el Plan Nacional de Seguridad Integral para el período 2014-2017 demuestra el constante cambio del concepto de seguridad integral. Así, se determinan las vinculaciones con el Plan Nacional del Buen Vivir que justifica su correlación en la conceptualización. Lo anterior, expone el alcance que se establece en el tema conceptual y la justificación de los lineamientos en las funciones institucionales. Entre los puntos destacados del Plan, están aquellos que se basan principalmente en la relación de los ciudadanos y las instituciones estatales. Como también, dentro de los nuevos tópicos que se presentan, se encuentran los concernientes a la ciberdefensa, tema que se desarrolla en la siguiente sección.

2.2. Alcance y ámbito de la ciberdefensa dentro del contexto de seguridad integral

La arquitectura de la seguridad y defensa se transforma de manera constante y como resultado sus instituciones, políticas y marco normativo. Ahora bien, dentro del contexto de la seguridad integral frente a los temas que se mencionan, en el Plan de Seguridad Integral 2011-2013 se introducen las acciones a desarrollarse en cuanto a estrategias, si bien se menciona que Ecuador establece sus amenazas, el ámbito científico y tecnológico, no analiza de manera profunda temas relacionados con la seguridad, defensa y gobernanza en el ciberespacio y en el internet, a pesar de que en América Latina ya se discutía sobre la gobernanza en las redes, es así el caso de que en 2007 se llevó a cabo en Brasil la segunda reunión de Foro de Gobernanza de Internet (Delgado, 2014). No obstante, en el Plan Nacional de Seguridad 2014-2017 se inicia a debatir y analizar temas como la ciberdefensa, ciberseguridad, ataques cibernéticos y el concepto político de las "guerras cibernéticas". Estos elementos son tomados en cuenta, ante las vulnerabilidades del Estado y la sociedad y los cambios entorno a los avances tecnológicos y científicos.

2.2.1. Marco legislativo desde el ámbito de la ciberdefensa

En lo que concierne al marco legal que involucra a la ciberdefensa cabe señalar que cada nivel del ciberespacio supone un ámbito legal y, en la esfera del constante cambio de la tecnología, el marco legal requiere la especialización (ciberlegislación) o adaptación de las leyes existentes (Delgado, 2014). En general, cada país tiene la capacidad jurídica, la competencia procesal y la jurisdicción para abordar las operaciones cibernéticas que afecten su seguridad y defensa (Nieto, 2014). En el caso de Ecuador, la construcción del sistema de ciberdefensa bajo el marco legal se desarrolla desde dos objetivos principales. El primero en la designación de responsabilidades y funciones de las Fuerzas Armadas y del Ministerio de Defensa Nacional, teniendo en cuenta la creación del sistema de Ciberdefensa. Así, se analiza la Constitución de la República, la Ley de Seguridad Pública y del Estado y la Ley Orgánica de la Defensa Nacional. En un segundo punto, se enfoca en la información como un activo que debe estar protegido en el contexto de la cibernética, entonces, se examina el Código Orgánico Integral Penal (COIP), la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y la Ley Orgánica de Telecomunicaciones (LOT) que contribuyen a la construcción de las condiciones jurídicas en el escenario de la ciberdefensa.

Abordando el primer punto, el marco normativo comienza en la Constitución de la República que contribuye a la defensa de la soberanía y establece el rol de las Fuerzas Armadas, en el artículo 158, que determina que "Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos. Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial (…)". (Constitución de la República del Ecuador, 2008, art. 158). Al respecto, la Ley Orgánica de Defensa Nacional incluye al Ministerio de Defensa Nacional y delimita las funciones de los organismos, es así, que en el artículo 3, delega al Ministerio los aspectos políticos-administrativos y, por otra parte, al Comando

Conjunto de las Fuerzas Armadas para ejercer en los asuntos militares-estratégicos dentro de la competencia territorial.

Al analizar el contenido de la protección de la seguridad estatal, se encuentra en la Ley de Seguridad Pública y del Estado el artículo 2 que prevé "(…) la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar (…)" (Ley de Seguridad Pública, 2009, art.2). Este artículo reconoce la importancia de la soberanía de la tecnología y los riesgos que derivan de las operaciones cibernéticas. Complementariamente, el artículo 43 presenta la protección de instalaciones e infraestructuras y menciona que el Ministerio de Defensa ante la inseguridad de los sectores estratégicos de origen público o privado dispone a las Fuerzas Armadas. Al respecto, se considera que los ataques cibernéticos que se dirigen a estos sectores sitúa en vulnerabilidad la seguridad del Estado. Del mismo modo, la defensa en el ámbito militar resulta condicionada a la ejecución y los resultados, puesto que depende de las TIC para el mando y control de operaciones (Polo, 2016).

Ahora bien, en relación al segundo punto, sobre el acceso a la información, la Ley Orgánica de Transparencia y Acceso a la Información Pública tiene como objetivo garantizar el derecho de la ciudadanía al acceso de la información, considerado como un modelo de participación democrática y se dirige a los funcionarios y organismos del Estado. Se basa principalmente en la reserva de información[31]. De este modo, los archivos públicos son accesibles con excepción de información que se encuentre clasificada como reservada o confidencial por temas de seguridad nacional. En el caso de las Fuerzas Armadas, las directivas controlan y aseguran la documentación militar calificada (Castro, 2015).

Lo expuesto en la LOTAIP tiene relación directa con el Código Orgánico Integral Penal que tiene como objetivo aproximarse a las amenazas que se presentan mediante los ataques cibernéticos. El COIP entra en vigencia en el mes de agosto del 2014 e incluye artículos vinculados a delitos contra la seguridad de los sistemas relacionados con las TIC. Desde el artículo 229 hasta el artículo 234

[31] Entre los que se encuentran: "estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc." (Espinoza & Verdezoto, 2015, p.30).

se encuentran los delitos correspondientes al tema (Castro, 2015). A continuación, se detallan:

Art. 229.- Revelación ilegal de base de datos

Art. 230.- Interceptación ilegal de datos

Art. 231.- Transferencia electrónica de activo patrimonial

Art. 232.-Ataque a la integridad de sistemas informáticos

Art. 233.-Delitos contra la información pública reservada legalmente

Art.234.-Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

En general, la pena se extiende de 3 años a 5 años y la máxima puede alcanzar hasta 7 años en el caso del artículo 232, pues requiere conocimientos avanzados en informática; adicionalmente, todas las sanciones contienen privación de libertad. Las leyes engloban la privacidad, el patrimonio, los datos informáticos y en si el valor de la información y la capacidad de acceso. También, es importante mencionar que el anterior Código Penal no contenía temas relacionados a los sistemas de información y comunicación. De acuerdo con Edwin Castro, Coronel de E.M.C., (2015) el Código no contempla ni abarca suficientes temas en el contexto donde la tecnología se transforma constantemente, no obstante, la legislación permite contrarrestar ataques vinculados a la información digital. Así, Juan Pablo Albán (2016), sugiere para el tema procesal penal que la investigación contenga una metodología específica para cada sanción, con un procedimiento diferenciado.

En el tema de seguridad, la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos promulgada desde abril de 2015 como se establece en el primer artículo regula temas relacionados con mensajes, firma electrónica, certificaciones, contrataciones, comercio y, en general, servicios electrónicos (Ley de Comercio, Firmas, Electrónicas y Mensajes de Datos, 2015). Además, establece que los mensajes de datos tienen valor jurídico similar a los documentos escritos. La importancia de esta ley recae en establecer herramientas jurídicas que reconozcan que el acceso y el uso de los servicios electrónicos se realizan en un entorno seguro.

Finalmente, la Ley Orgánica de Telecomunicaciones vigente desde febrero del 2015 tiene este objetivo que se expone en el artículo 1: "desarrollar, el régimen general de telecomunicaciones y el espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajos los principios y derechos constitucionalmente establecidos". En Ecuador, bajo la nueva Ley Orgánica de Telecomunicaciones se crea la Agencia de Regulación y Control de las Telecomunicaciones (Arcotel) que absorbe a la Supertel, la Conatel y la Senatel (Duarte, 2015). En el artículo 142 se establece como la entidad encargada de la administración y regulación de las telecomunicaciones y el espectro técnico de medios de comunicación social. Este último vinculado a la gobernanza de internet.

En general, la promulgación de la Ley de Comercio Electrónico constituye uno de los avances en el tema, además, del Código Orgánico Integral Penal (COIP), permite neutralizar las amenazas y aplicar las sanciones pertinentes (Sosa, 2014). Las leyes citadas han introducido diferentes temas relacionados con el ciberespacio y la ciberdefensa, no obstante, la complejidad de los ataques y amenazas cibernéticas sugiere limitaciones en la aplicación e implementación de los procesos legales.

2.2.2. Estructura institucional

La estructura institucional en materia de ciberdefensa en Ecuador se instituye como la convergencia de distintas instituciones, pues no existe una que centralice los temas relacionados a la ciberdefensa (Paredes, 2016). En el escenario planteado, la ciberdefensa se encuentra dentro del Sistema de Defensa Nacional y se considera un elemento fundamental para mantener la Seguridad Integral, pues, se reconoce la importancia de la protección de la información estratégica, la infraestructura crítica del país, las redes e información electrónica y el bienestar de la ciudadanía (Agenda Política de Defensa Nacional, 2014). En esta línea, se encuentran diferentes elementos de análisis, en un primer momento, el rol de cada una de las instituciones a cargo de la planificación, desarrollo de conceptos y lineamientos estratégicos.

La Defensa parte del "control, cuidado y protección del espacio territorial" (Agenda de la Política de la Defensa, 2014, p.29). En la Agenda Política de la Defensa 2014-2017, se reconoce un nuevo dominio apartado de los espacios tradicionales (terrestre, marítimo y aéreo) y, que adquiere importancia desde la perspectiva histórica como un elemento esencial en la seguridad del Estado y de sus ciudadanos, que se dirige en el dominio denominado "ciberespacio", como resultado, en materia de defensa se instaura la "ciberdefensa". Cuando se establecen los primeros lineamientos entorno al concepto de la ciberdefensa, el primer elemento que se considera es la delimitación del concepto desde el punto institucional. En el glosario referencial de la Agenda Política de la Defensa (2014-2017) y en el Manual de Operaciones de Información del Comando Conjunto de las Fuerzas Armadas (COMACO) (2011) se establece que la ciberdefensa:

> Constituye una iniciativa diseñada para ampliar los sistemas de defensa de los Estados y protegerlos de los nuevos riesgos emergentes en la sociedad de la información. Entre estos riesgos se encuentran la "guerra cibernética", entendida como la utilización de las debilidades de las redes informáticas que van desde el espionaje y la infiltración de los sistemas informáticos hasta la destrucción física de los recursos del oponente; y el "espionaje cibernético" cuyo objetivo es obtener información confidencial circulante en ese medio. La Ciberdefensa es fundamental en este momento, en el que se han visto las enormes consecuencias que este tipo de ataques pueden generar a la seguridad del Estado. (Agenda Política de la Defensa, 2014, p.94)

La estructura del concepto propone la transformación de los sistemas estatales de defensa y, ubica al Estado y sus instituciones como responsables y como protectores de las nuevas amenazas y riesgos, en tal sentido, presenta varios conceptos como la "guerra cibernética" y el "espionaje cibernético" delimitando las operaciones que ponen en riesgo la seguridad estatal, con preponderancia a nivel de un escenario bélico. Roque Moreira (2014), Rector de la Universidad de las Fuerzas Armadas (UFA-ESPE) menciona que paralelamente al surgimiento del concepto de ciberdefensa, se analizan y se destinan actividades técnicas,

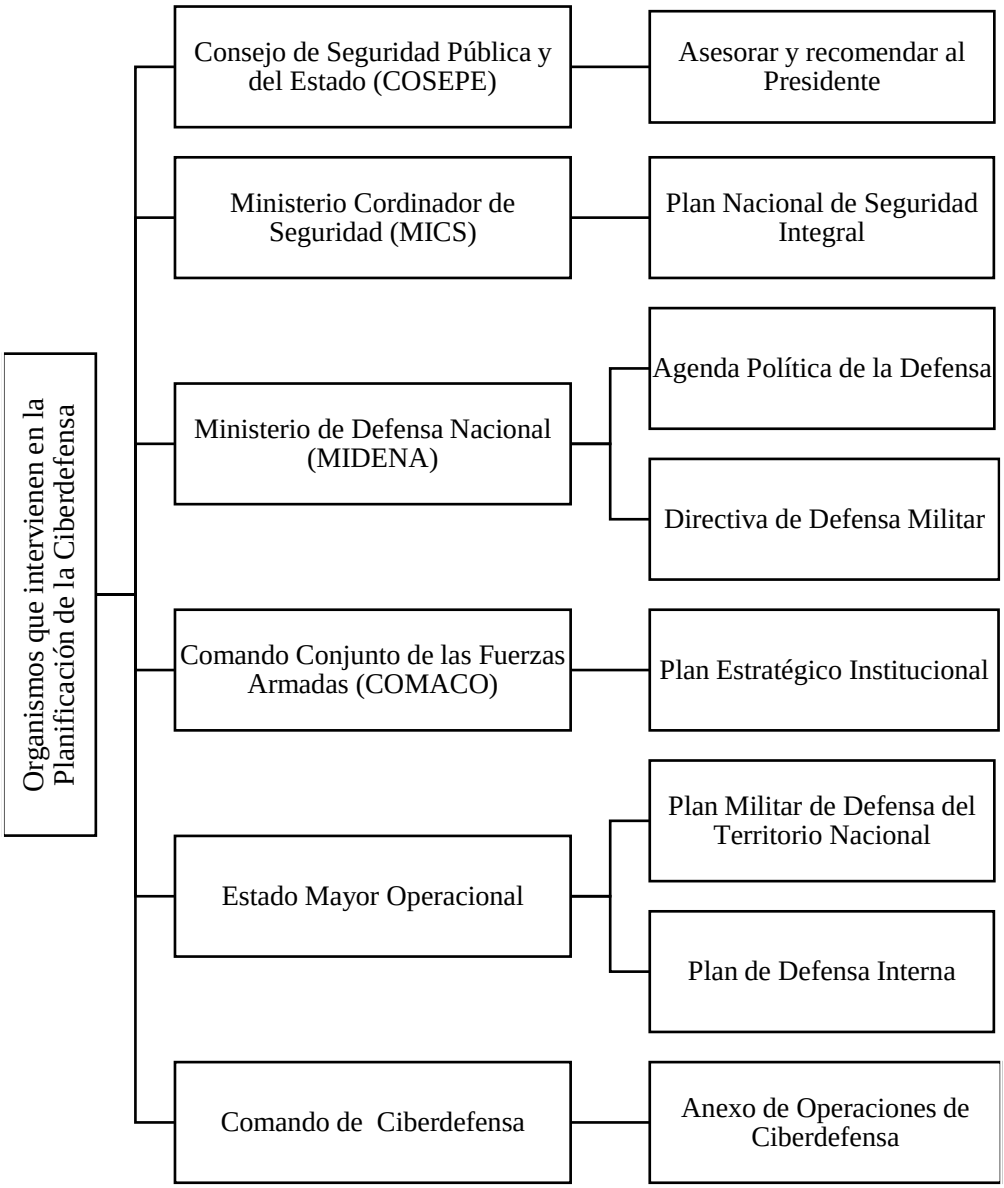
estrategias y tácticas en la seguridad de los sistemas del Estado y de sus instituciones.

En este panorama, en el tema de la ciberdefensa en concordancia con la Agenda se encuentran dos instituciones a cargo: el Ministerio de Defensa Nacional y las Fuerzas Armadas, y se excluye al Ministerio de Relaciones Exteriores y Movilidad Humana[32] que se direcciona en otros tópicos del espectro de la defensa, sin embargo, coordina interinstitucionalmente para evitar la filtración de información. Sobre lo mencionado, el rol de las Fuerzas Armadas se presenta como prioritario en el caso de la ciberdefensa es así, que en la Agenda se proponen cuatro misiones complementarias para el período 2014-2017. La primera misión es: "Garantizar la defensa de la soberanía e integridad territorial". (p.40). En esta misión específicamente se encuentran las operaciones de protección del espacio cibernético, esto implica que se les atribuye a las Fuerzas Armadas el aspecto operativo. Por otro lado, la función del Ministerio de Defensa Nacional frente a este tema es velar las capacidades operativas y desarrollar las políticas específicas en el ámbito de la ciberdefensa. Así, a través de la figura 1 se detallan los organismos que intervienen en la planificación.

[32] El Ministerio de Relaciones Exteriores y Movilidad Humana es el rector de la política internacional, la integración latinoamericana y movilidad humana (Ministerio de Relaciones Exteriores y Movilidad Humana, s.f.).

FIGURA 1

ORGANISMOS QUE INTERVIENEN EN LA PLANIFICACIÓN DE LA CIBERDEFENSA



Fuente: La Ciberdefensa en el Contexto de la Agenda Política de la Defensa, 2014
Elaborado por: Byron Freire (2014)

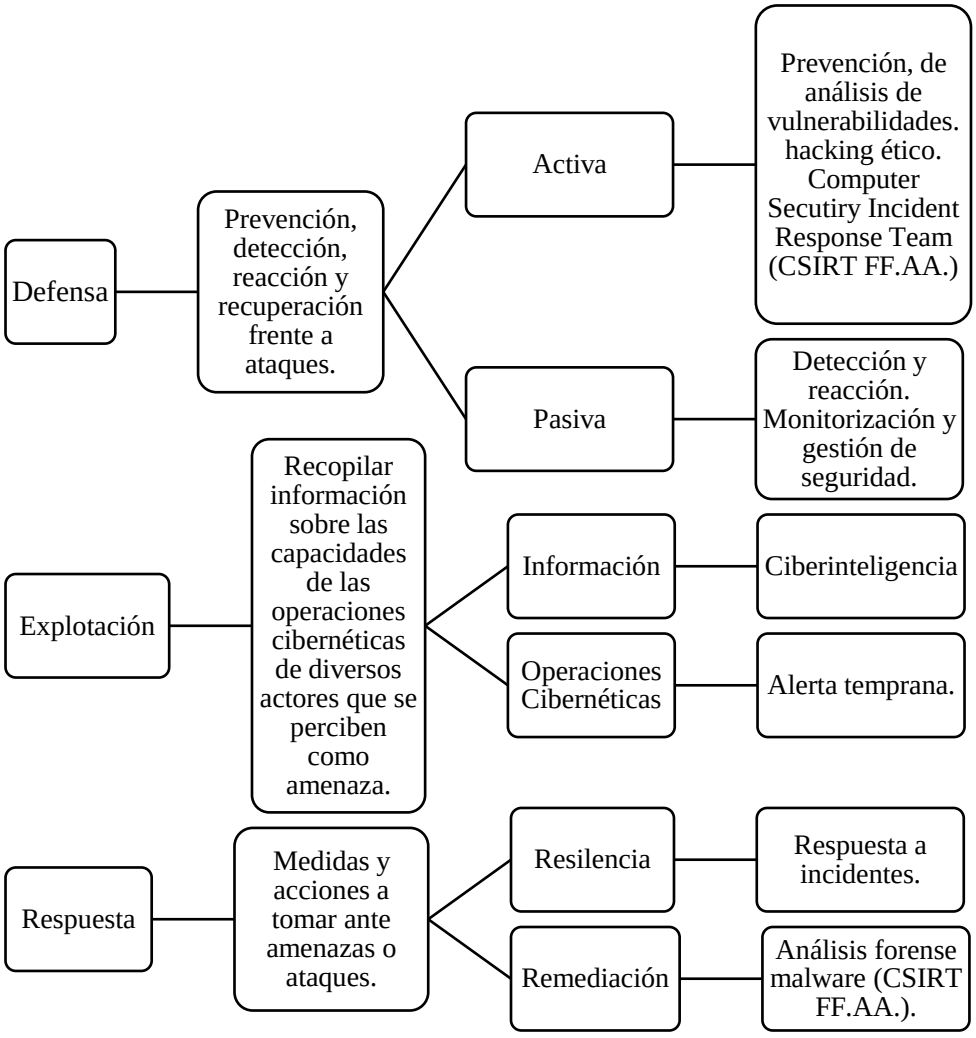
Siguiendo con el análisis, se implementa en el año 2015 con un presupuesto de ocho millones de dólares el Comando de Ciberdefensa[33] perteneciente al Comando Conjunto de las Fuerzas Armadas, considerado el sexto Comando y el primero en el tema. En este marco, las capacidades estratégicas del Comando se derivan del trabajo en conjunto de los diversos organismos que

[33] Acuerdo Ministerial No. 281, 12 de septiembre de 2014 (Vargas, Recalde, & Reyes, 2017).

pertenece a las Fuerzas Armadas en concordancia con el Plan Estratégico Institucional (2010-2021), Plan Militar de Defensa del Territorio Nacional y Plan de Defensa Interna. El Comando de Ciberdefensa con el objetivo de preparar y fortalecer las operaciones cibernéticas que garanticen la seguridad del Estado y el derecho de la ciudadanía a la paz y el desarrollo, extiende su misión a tres ámbitos: defensa, explotación y respuesta (Paredes, 2016).

FIGURA 2

ESTRUCTURA ORGANIZACIONAL POR PROCESOS DEL COMANDO DE CIBERDEFENSA



Fuente: La Ciberdefensa en el Contexto de la Agenda Política de la Defensa, 2014
Elaborado por: Byron Freire (2014)

El Comando de Ciberdefensa como se observa en la figura 2 realiza diversos procesos con el fin de cumplir la misión establecida. En general, la estructura organizacional por Procesos del Comando de Ciberdefensa analiza varios aspectos de las operaciones cibernéticas y se enfoca principalmente en la prevención y en la reacción frente a los ataques y amenazas. Además, se destacan varios conceptos técnicos, en el ámbito de defensa activa se menciona el concepto de *hacking ético*[34] y en la respuesta y remediación se encuentra el análisis forense "malware"[35]. La gestión operativa desde esta estructura se centra en ejes de educación del personal, infraestructura y la adquisición de softwares.

Conjuntamente, el Comando se ha orientado en cuanto a la defensa del Estado en las infraestructuras críticas, ante este concepto se puede definir que "son las instalaciones, sistemas y servicios, que están presentes en las actividades bancarias, financieras, generación de energía, transporte, comunicaciones, entre otras, cuya afectación causa un grave daño en varios ámbitos, tales como el psicosocial, político, económico y militar" (Sosa, 2014, p.89). En el contexto de Ecuador, se pueden considerar refinerías, hidroeléctricas, instituciones de comunicación y en sí sistemas y dispositivos del Estado (Sosa, 2014).

A partir de esta visión y ejecución de las instituciones desde sus respectivas funciones, se plantea que Ecuador debe estar preparado para enfrentar amenazas externas que atentan contra la democracia, el bienestar estatal y de los ciudadanos con referencia a los ataques cibernéticos. Dentro de las observaciones que se han realizado, cabe mencionar que la ciberdefensa es un tema transversal, por lo tanto, las diferentes instituciones del Estado deben ejecutar acciones en torno a la defensa cibernética. Es así, el caso de la Secretaría de la Inteligencia, que de acuerdo a la disposición de la Ley de Seguridad Pública del Estado no tiene incursión en la ciberdefensa, no obstante, debe ejecutar acciones ante las amenazas cibernéticas (Cordero, 2015).

[34] Hacking ético "consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos (…)" (Alejandro Reyes Plata, 2010, p.1). Por otro lado, el "hacker" es la persona que se encuentra involucrada en modificación mediante técnicas de las características de un sistema (Satapathy & Ranjan, 2015).

[35]El término malware "proviene del término en inglés malicious software, y partiendo desde su concepto, puede referirse como cualquier archivo (programa, código, documento, mensaje, imagen) creado con el objetivo de causar prejuicios sobre a información, reflejado en los usuarios de sistemas informáticos" (Pablo Gaviria, 2016, p.16).

2.2.3. Una nueva agenda: políticas públicas

Los conceptos definidos por las instituciones responsables son la fuente de las políticas públicas, por lo tanto, es esencial que las definiciones sean delimitadas y claras para cumplir con los propósitos, objetivos, estrategias y directrices (Chávez, 2016). Así, conceptos como la seguridad integral, ciberdefensa y otros términos relacionados orientan las políticas del gobierno que tienen efecto en el aparato estatal y la ciudadanía. En este sentido, en Ecuador se puede mencionar las políticas provenientes del Plan Nacional del Buen Vivir (Secretaria Nacional de Planificación y Desarrollo), el Plan Nacional de Seguridad Integral (Ministerio Coordinador de Seguridad) y la Agenda Política de la Defensa (Ministerio de Defensa Nacional).

A partir de la articulación de las instituciones y conceptos, el Ministerio de Defensa Nacional presenta la Agenda Política de la Defensa (2014-2017) y realiza la Matriz de Objetivos, Políticas y Estrategias (2013-2017), que a continuación, se detallan y se desarrollan las políticas en referencia a la ciberdefensa:

TABLA 2

OBJETIVOS, POLÍTICAS Y ESTRATEGIAS PARA LA CIBERDEFENSA 2013-2017

Objetivos del PNBV	
Objetivo 12. Garantizar la soberanía y la paz, profundizar la inserción estratégica en el mundo y la integración latinoamericana.	
Políticas del PNBV	
12.5 Preservar la integridad territorial del Estado y sus soberanías, en el marco de estricto respeto de los derechos humanos.	
Ejes Articuladores del PNSI	
Soberanía e Integración	Soberanía e Integración y Cultura de Paz

Políticas del PNSI	
Política 3. Garantizar la soberanía, integridad territorial e integración regional y mundial para promover relaciones de cooperación, pacíficas y de mutua confianza en el marco del Buen Vivir.	Política 6. Promover la cultura de uso de la inteligencia estratégica para la gestión de la Seguridad Integral en el marco del Buen Vivir.
Objetivos de la Defensa	
GARANTIZAR LA DEFENSA DE LA SOBERANÍA E INTEGRIDAD TERRITORIAL Y PARTICIPAR EN LA SEGURIDAD INTEGRAL	
Política de la Defensa	
1) GARANTIZAR LA SOBERANÍA E INTEGRIDAD TERRITORIAL PARA LA CONSECUCIÓN DEL BUEN VIVIR, EN EL MARCO DE LOS DERECHOS HUMANOS.	4) PROTEGER LA INFORMACIÓN ESTRATÉGICA DEL ESTADO, EN MATERIA DE DEFENSA.
Estrategias	
3. Desarrollar capacidades para la ciberdefensa.	1) Proteger la infraestructura, redes estratégicas e información electrónica, en el ámbito de la Defensa. 2) Desarrollar la capacidad de ciberdefensa. 3) Fortalecer los mecanismos interinstitucionales para hacer frente a las amenazas cibernéticas que atentan contra la seguridad del Estado. 4) Participar en las iniciativas de Unasur para alcanzar la seguridad de las telecomunicaciones suramericanas.

Fuente: Agenda Política de la Defensa Nacional, 2014-2017
Elaborado por: Ministerio de la Defensa Nacional (2014)

Bajo este enfoque, el Plan Nacional del Buen Vivir (2013-2017) establece las primeras políticas en concordancia con sus objetivos y en el contexto de la seguridad integral se guían las acciones sectoriales que derivan en objetivos, políticas de la ciberdefensa y estrategias. Las prioridades de las políticas se orientan principalmente en el tema de soberanía, desde la perspectiva del buen vivir, los derechos humanos y la paz. A la vez, la soberanía se considera como una concepción multidimensional, donde el factor de la ciberdefensa se encuentra en el centro y requiere, como se establecen en las estrategias "desarrollar las capacidades". Por lo expuesto y regresando al primer capítulo la soberanía se dirige al dominio del ciberespacio que comprende diversos niveles de alcance.

Para consolidar el compromiso con la información del sistema estatal se encuentra la política de "proteger la información estratégica del Estado en materia de Defensa". El Gobierno Nacional se ha enfocado en establecer políticas estatales en relación a la seguridad cibernética que englobe todo el aparato estatal. Por una parte, en el tema de la ciberseguridad mediante la Secretaría Nacional de la Administración Pública (SNAP)[36], se han determinado directrices en las que todas las entidades públicas están obligadas con el cumplimiento de las normas técnicas para seguridad de la información vital del Estado (Sosa, 2014). Es el caso del Acuerdo No. 166 de la SNAP, las entidades tuvieron hasta el mes de marzo de 2015 para implementar su funcionamiento y se trata del Esquema Gubernamental de Seguridad de la Información (EGSI), en concordancia con las Normas Técnicas Ecuatorianas NTE-INEN-ISO/IEC 270 (Cordero, 2015).

Considerando la integración territorial se demuestra desde el PNBV, que el proceso de integración se perfila dentro de la agenda latinoamericana, igualmente, las intenciones regionales se muestran en la mención del organismo de la Unión de Naciones Suramericanas (Unasur). Esta iniciativa bajo la percepción de la interdependencia de los países y de las vulnerabilidades que presentan como región ante actores que han avanzado en el tema y cuentan con el dinamismo tecnológico apropiado.

Se puede identificar que las políticas comprenden las instituciones coordinadoras, articuladoras y ejecutoras. Además, existen políticas intersectoriales y sectoriales que direccionan las estrategias de acción en el campo de la ciberdefensa. En efecto, es necesario agregar organismos internacionales como la UNASUR ante el proceso de integración regional. En razón de ser un tema en construcción, existe la posibilidad de rectificar, modificar o agregar políticas que se adaptan al entorno mutable de los actores y amenazas.

[36] La misión de la SNAP es "mejorar la eficiencia en la gestión institucional de las entidades que conforman la Administración Pública Central y que dependen de la Función Ejecutiva mediante el diseño e implantación de políticas, normas y herramientas en materia de gestión por procesos, calidad de los servicios, control y evaluación de la gestión, gobierno electrónico e imagen gubernamental" (Secretaria Nacional de Administración Pública, s.f.).

2.3. Infraestructura tecnológica de la ciberdefensa, gobernanza de internet y la visión regional desde la Unasur

La estructura de la ciberdefensa como se ha establecido se compone de diversos elementos que hacen posible su aplicación en materia estatal. En este sentido, el debate se origina en la aplicación y operatividad, por lo tanto, es necesario considerar el aspecto técnico que a través de herramientas se conforma la infraestructura tecnológica. En el caso de Ecuador, las Fuerzas Armadas son responsables del ámbito operativo de la ciberdefensa.

Por otra parte, la complejidad de abordar la ciberdefensa deriva la discusión al tema de internet, que se considera como una plataforma del ciberespacio. La relación existente entre éste y el Estado se centran en la gobernanza, como parte del proceso de toma de decisiones, además, vinculado a vigilar y controlar amenazas que surgen en este ámbito. Finalmente, considerando el tema regional y su importancia debido principalmente a la orientación de las políticas a la integración latinoamericana, la Unasur se presenta como un ente que propone una alternativa y ampliación de los avances en concordancia con la ciberdefensa.

2.3.1. Infraestructura básica: herramientas que fortalecen a la ciberdefensa

La posesión de infraestructura tecnológica y la sistematización de los componentes del ciberespacio en el ámbito técnico suponen mecanismos de colaboración, que se destacan y aportan las cibercapacidades de defensa de los Estados. En los elementos a considerar en el desarrollo de la infraestructura se encuentra el aporte presupuestario**,** políticas, legislación, directrices y estrategias. Desde esta perspectiva, en el caso de Ecuador las infraestructuras en el ámbito nacional se destacan el CERT ARCOTEL (EcuCERT), la Policial Judicial y la Fiscalía General del Estado, todos enfocados en la ciberseguridad. En relación a la ciberdefensa, la situación es diferente debido al contexto ambiguo en el que se desarrolla (Vargas, Recalde, & Reyes, 2017).

En 2014 se crea EcuCERT, Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de Telecomunicaciones del Ecuador (ARCOTEL). El EcuCERT (2014) tiene como objetivo brindar a su Comunidad Objetivo[37] soporte en temas de seguridad informática. Adicionalmente, contribuye a la seguridad del uso del internet y aporta al uso seguro de las redes para la comunidad (EcuCERT, 2014). En cuanto a la Policía Judicial del Ecuador, el Ministerio del Interior informó a través de su portal digital en 2012 la creación de la Unidad de Investigación de Cibercrimen. El objetivo se orienta en "detectar, identificar, localizar y neutralizar el accionar de las personas con estas conductas ilícitas, a través del uso de la tecnología" (Espinoza & Verdezoto, 2015, p.53). El proceso para que la ciudadanía se beneficie de los servicios, consiste en acudir a la Fiscalía, para que la Policía Judicial direccione el tema a los expertos informáticos.

Adicionalmente, la Fiscalía General del Estado crea en 2008 el Departamento de Delitos Informáticos y Análisis Forense, con el propósito de proteger a los usuarios del internet de la criminalidad informática y las vulnerabilidades de los sistemas (Espinoza & Verdezoto, 2015). Por último, se conformó el Centro de Operaciones Estratégico Tecnológico, con el objetivo de monitorear ataques informáticos sobre los dispositivos de diferentes instituciones públicas (Vargas, Recalde, & Reyes, 2017). Desde 2013, el Centro en conjunto con la Secretaría de la Inteligencia se han encargado del monitoreo de equipos de seguridad de varias instituciones gubernamentales (Secretaría de la Inteligencia , 2014).

Paralelamente a lo establecido en el Plan Nacional de Seguridad Integral y la Agenda Política de la Defensa se encuentra el Comando de Ciberdefensa. No obstante, hasta el momento no se encuentra claramente en registros la infraestructura crítica. En este escenario ambiguo, las instituciones han empleado y propuesto iniciativas en diversos ámbitos relacionados a la infraestructura, la

[37] La Comunidad Objetivo está conformada por: "ARCOTEL, prestadores de servicios de telecomunicaciones y, con autorización previamente solicitada a la máxima autoridad, las instituciones del sector público y privado que requieran sus servicios" (EcuCERT, 2014).

interconectividad y asuntos vinculados a la tecnología, portales, sistemas y, en general recursos que aportan a las instituciones (Vargas, Recalde, & Reyes, 2017).

En efecto, los esfuerzos dirigidos a la ciberdefensa y también a la ciberseguridad mediante iniciativas específicas tanto públicas como políticas gubernamentales, han sido limitadas y su efectividad condicionada, como resultado persiste la existencia de vulnerabilidades. Así en el contexto planteado, al tener en cuenta la normativa y las políticas públicas todavía no se logran consensos en criterios técnicos-metodológicos en relación a estándares, roles de los actores, metas y procesos en el uso de tecnologías (Vargas, Recalde, & Reyes, 2017).

2.3.2. Un espacio de la ciberdefensa: acercamiento a la gobernanza de internet en Ecuador

La participación de Ecuador en el debate sobre la gobernanza del internet desde el 2013, se llevó a cabo, en octubre en la reunión número 24 del Consejo de Derechos Humanos, en la cual Paquistán propuso a título de Ecuador y otros países la elaboración de un mecanismo intergubernamental de gobernanza de internet. En 2014, Fadi Chehadi, presidente de la Corporación de Internet para la Asignación de Nombres y Números[38] (ICANN, por sus siglas en inglés) y Dilma Rousseff, presidenta de Brasil comenzaron el desarrollo de la iniciativa NETmundial[39] donde se registró presencia de distintos actores de Ecuador, entre ellos el sector privado, público y sociedad civil (Delgado, 2014).

En este contexto, el 27 de noviembre de 2014 se realizó en Quito el "Encuentro Nacional de Gobernanza de Internet"[40], el evento se caracterizó por ser el primero sobre el tema y reunió actores provenientes del gobierno, activistas y coaliciones de la sociedad civil y expertos internacionales. El encuentro se

[38] La ICANN es una organización internacional que coordina el sistema global de identificadores únicos de internet (ICANN, s.f.).
[39] El objetivo de la iniciativa NETmundial es crear un espacio de innovación para desarrollar soluciones en temas de gobernanza de internet (NETmundial, s.f.).
[40] El encuentro fue organizado por el "Centro de Estudios Superiores de Comunicación para América Latina (CIESPAL), la Asociación para el Progreso de las Comunicaciones (APC), la Asociación de Software Libre del Ecuador (ASLE), la Red Infodesarrollo, FLOK y la Agencia Latinoamericana de Información (ALAI)" (FLOK Society , 2014).

definió como una plataforma de debate, sensibilización y reflexión en el contexto regional y global, dentro del marco de los derechos humanos. El objetivo principal fue la contribución orientada al desarrollo fundado en el interés público mediante un proceso participativo de la gobernanza del internet (FLOK Society , 2014). Este hecho, marca el comienzo de un nuevo análisis de la gobernanza de internet en Ecuador, entonces, para abordar esta temática el texto se dividió en infraestructura, acceso y uso y contenidos.

La capa de la infraestructura física del internet, se considera un conjunto de componentes técnicos como estructuras, protocolos y estándares. La dificultad de aproximarse a este tema se debe a la condición territorial y extraterritorial del internet. En cuanto a la infraestructura en telecomunicaciones, ésta abarca diferentes medios como telefonía, fibra óptica entre otros, cada uno de los elementos comprende un cuerpo legal. Las regulaciones a nivel internacional se encuentran bajo la responsabilidad de la Unión Internacional de Telecomunicaciones (Delgado, 2014). En Ecuador, el ente a cargo es la Agencia de Regulación y Control de las Telecomunicaciones. El acceso a nivel internacional desde el país se realiza mediante tres cables submarinos: Telefónica International Wholesale Service (TIWS), Panamericano (PanAm) y Pacific Caribbean Cable Systems (PCCS). En el caso, del TIWS y el PCCS llegan a Florida (Estados Unidos) y el Pan-Am termina en las Isla Vírgenes Americanas del Caribe, estos tres cables permiten que la velocidad en internet aumente en 325Gbps[41] y se reduzcan los costos (Ministerio de Telecomunicaciones y Sociedad de la Información, 2016).

Así también, el análisis de la dimensión temporal de algunos indicadores de infraestructura en telecomunicaciones, señala que la extensión de la fibra óptica, de acuerdo al Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) en 2013 fue de 31.000 km y en 2016 alcanza 71.0000 km. Como resultado de estos datos, uno de los sectores que se ha beneficiado es el móvil, la cobertura poblacional de telefonía a nivel nacional en el mismo orden de años es de 96,58% y 97%. Temas relacionados a los estándares globales como el

[41] En el año 2013 la velocidad alcanzaba los 147,8Gbps (Ministerio de Telecomunicaciones y Sociedad de la Información, 2016).

Protocolo de Internet (IP, por sus siglas en inglés), el Sistema para Nombres de Dominio[42] (DNS, por sus siglas en inglés), son componentes de funcionamiento que se encuentran concentrados por la ICANN, que en 2016 concluyó su contrato con el Departamento de Comercio de Estados Unidos que mantenía un rol vigilante, la transición se delega a un grupo interdisciplinario de la comunidad internacional (El Telégrafo , 2016).

El internet no solo se centra en la composición de asuntos técnicos para su operación, sino también el debate debe dirigirse al uso, el acceso y los contenidos. Existe un incremento en relación al acceso y uso de internet, desde un panorama global, la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) estima que para 2020, el número de dispositivos interconectados a la red, será seis veces mayor al número de personas (Nieto, 2014). En Ecuador la regulación del sector de las telecomunicaciones en concordancia con la LOT, instaura el acceso a Internet como un servicio básico (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2016). Por consiguiente, en la tabla a continuación se presentan indicadores de referencia:

TABLA 3

INDICADORES DE ACCESO Y USO 2013-2016

Indicador	2013	2014	2015	2016
Personas que usan TIC	44,79%	48,58%	51,82%	56,87%
Personas que usan computadora	43,56%	47,52%	50,06%	52,43%
Personas que han usado Internet	40,35%	46,35%	50,48%	55,63%
Analfabetismo digital (15 a 49 años)	20,04%	14,43%	12,22%	11,45%
Hogares con acceso a internet	28,27%	32,44%	32,80%	36,03%
Hogares que tienen computador (escritorio-laptop)	35,70%	37,50%	40,84%	42,35%

Fuente: Observatorio TIC, MINTEL, 2016
Elaborado por: Cristina Salinas

[42] El DNS permite a los usuarios navegar en internet, las computadoras poseen una dirección única o IP compuesta por números, mediante el DNS se proporciona el uso de letras, por ejemplo: www.iccan.org en lugar de "192.0.34.163" (Vera & Tamayo, 2010).

Los datos expuestos demuestran un crecimiento en cuanto al uso de TIC, computadoras e internet tanto de personas como hogares, es decir, la población no se ha detenido en ingresar a la tecnología y adquirir conocimientos para utilizarla a través de sus diferentes dispositivos, en particular computadoras y móviles. Además, al analizar el incremento se destacan diversas razones: la creación del Plan Nacional de Gobierno Electrónico (2014-2017)[43], la creación de redes comunitarias[44] de zonas rurales y urbano marginales y políticas que se han enfocado en el cambio productivo y el desarrollo del país (Vargas, Recalde, & Reyes, 2017). De este modo, se plantean dos escenarios, el primero, se distingue como un potencial espacio para expandir amenazas y operaciones cibernéticas que atenten contra a seguridad y defensa del Estado, segundo, el crecimiento de usuarios también, representa que la estructura de la defensa y seguridad debe abarcar varios aspectos del internet para proporcionar un espacio seguro apegado al cumplimiento de los derechos humanos.

El contenido que se encuentra en internet, regula a los medios digitales de personería jurídica obtenida en Ecuador que distribuyan contenidos informativos y de opinión y tienen los mismos derechos y obligaciones establecidos en la LOT que los medios de comunicación social. Sin embargo, en el artículo 2 establece que "los contenidos que formulen ciudadanos y las personas jurídicas en sus blogs, redes sociales y páginas web personales, corporativas o institucionales". Estos últimos temas todavía se presentan como pendientes pues no han sido analizados como un aspecto que repercute en diferentes ámbitos. Al considerar se mencionan los avances, en cuanto a iniciativas el 23 de mayo de 2017 se presentó el Proyecto de Ley que Regula los Actos de Odio y de Discriminación e Internet[45], tiene 10 artículos que se destinan a empresas proveedoras de servicios que funcionan a través de comunicaciones telemáticas, plataformas de internet. Los proveedores de servicio de redes sociales deberán elaborar un informe trimestral sobre la

[43] El Plan de Gobierno Electrónico es dirigido y gestionado por la Secretaría Nacional de la Administración Pública y, tiene como objetivo conectar y acercar el gobierno al ciudadano a través de la tecnología, de una manera tangible y práctica que impulse la innovación e interacción entre actores del gobierno electrónico dentro del marco de los servicios públicos (Secretaría Nacional de la Administración Pública, 2014).
[44] El acceso a internet se realiza a través de implementación de infocentros, laboratorios escolares y aulas móviles de capacitación (Agencia Pública de Noticias del Ecuador y Suramérica , 2014).
[45] El proyecto fue presentado por el presidente de turno Rafael Correa

gestión de reclamos o reportes sobre el contenido ilegal, y se presentarán al Ministerio de Justicia en un plazo de 15 días. (Gonzáles, 2017)

Como se ha establecido el espectro de temas de la gobernanza de internet se extiende a distintas aristas, por lo tanto, el texto no analiza todas las áreas de igual importancia. El objetivo es demostrar la complejidad que implica el tratamiento de los temas que se encuentran vinculados al internet y de la multiplicidad de aplicaciones que engloba. No obstante, la gobernanza de internet tiene relación con la ciberdefensa en contrarrestar operaciones cibernéticas o amenazas que afectan la seguridad de la información e instituciones del Estado.

2.3.3. La situación de la ciberdefensa en el ámbito regional: Unasur

La ciberdefensa y ciberseguridad se han considerado temas relevantes en organismos globales y regionales, en concordancia con diversas resoluciones de la Asamblea General de las Naciones Unidas que promueven a los Estados miembros analizar las amenazas que afectan la seguridad de la información. En el ámbito regional, el tema del ciberespacio como prioridad se enfocó en establecer un marco jurídico dirigido en lo penal y planteó regulaciones que se direccionaron en el aspecto tecnológico y comercial con el objeto de beneficiar el desarrollo de los países. En el caso de Suramérica, en concordancia con los distintos tipos de regionalismo[46], se origina la Unasur[47] como propuesta a una integración política y social, y subordinada de tópicos comerciales. La agenda multidimensional con un liderazgo político de los Jefes de Estado, aborda temas concernientes a seguridad nacional y regional y, establece el Consejo de Defensa Suramericano (CDS) (Aranda, Riquelme, & Salinas, 2015).

La creación del Consejo de Defensa Suramericano en 2008, que se encarga de la implementación de políticas de defensa en los ámbitos de cooperación

[46] El regionalismo para Atkins (1991) parte de un subsistema que es "un conjunto de Estados geográficamente próximos que interactúan regularmente y comparten hasta cierto punto un sentido de identidad regional, reconocido por los actores exteriores" (Aranda, Riquelme & Salinas, 2015, p.106).
[47] Posteriormente al origen de la Unasur, se establece la Comunidad Suramericana de Naciones (CSN) en 2004 en la Reunión de Presidentes de América del Sur en Perú. Consecutivamente, en 2007 en la Cumbre Energética Suramericana en Venezuela se cambia el nombre a Unión de Naciones Suramericanas (Unasur). El Tratado Constitutivo entra en vigencia en 2011 (Unión de Naciones Suramericanas, s/f).

militar, acciones humanitarias, operaciones de paz, tecnología y educación (Unión de Naciones Suramericanas , 2008). En conjunto con el Consejo Suramericano de Infraestructura y Planeamiento (Cosiplan)[48] y consejos ministeriales, evalúan el avance de proyectos sobre defensa cibernética y promueve la inclusión digital de telecomunicaciones e interconexión de redes de fibra óptica. Así, en 2013 acordaron los ministros de telecomunicaciones construir en mega-anillo de fibra óptica de 10.000 kilómetros, con el fin de limitar el paso de las telecomunicaciones de América Latina a territorios extra regionales (Tamayo, 2013). Pues, en la declaración del 2013 la Unasur rechaza:

> Firmemente la intercepción de las telecomunicaciones y las acciones de espionaje a nuestros países por parte de la agenda nacional de seguridad del gobierno de Estados Unidos, o sea quien fuere que la ejecute, las cuales constituyen una amenaza a la seguridad y graves violaciones de los derechos humanos, civiles y políticos del derecho internacional y de nuestras soberanías, y dañan las relaciones entre naciones (Tamayo, 2013, p.97).

Pablo Celi (2013) subdirector del Centro de Estudios Estratégicos de Defensa (CEED), respecto a la construcción añade que se trata principalmente sobre el aspecto político como una estrategia regional que se reflejará en el sistema administrativo y jurídico y, el ámbito técnico contribuye a que el proyecto avance y sea factible en el tiempo. La importancia de este proyecto recae en el análisis de Raúl Zibechi (2011), que expone la ruta de un mail enviado entre Rio Branco (Brasil) y Puerto Maldonado (Perú), pues en el ejemplo propuesto señala que el mail recorre Brasilia, Fortaleza, Miami, California, Lima y finalmente Puerto Maldonado, en efecto, en lo que podrían ser 300 kilómetros la ruta se expande debido a la dependencia tecnológica que se vinculan a las vulnerabilidades de los países de la región (Quintero, 2014).

[48] El Consejo Suramericano de Infraestructura y Planeamiento se creó en 2009 y tiene como objetivos: primero, la integración de la infraestructura regional, y segundo, la construcción de redes de transportes y telecomunicaciones (Unión de Naciones Suramericanas, s/f).

Además, se han desarrollado diferentes propuestas, en 2014 se realizó el Seminario Regional sobre Ciberdefensa en Argentina que responde a lineamientos del Plan de Acción 2014 para contribuir a la defensa de amenazas cibernéticas y se abordaron temas en relación a las infraestructuras críticas, seguridad de la información y comunicaciones, ecosistemas informáticos, entre otros. Paralelamente, en la tercera reunión del Grupo de Trabajo de Ciberdefensa, se acordó la creación del foro regional de Grupo de Trabajo de Ciberdefensa, el intercambio de información, concretar procedimientos de la red de contactos y analizar definiciones conceptuales de ciberdefensa y ciberseguridad (Justribó, 2014).

La posición de Ecuador frente al tema se manifiesta en las políticas y estrategias establecidas, pues en la Agenda de Política de la Defensa 2014-2017 analizada en la subsección anterior sobre este tema, se enfatiza en la participación del país en las iniciativas del bloque regional en la seguridad de las telecomunicaciones. En 2014 en la I Declaración de Cartagena de la Reunión de Ministras y Ministros del Consejo de Defensa Suramericano, María Fernanda Espinosa, Ministra de Defensa de Ecuador mencionó:

> nos hemos propuesto avanzar en la ciberdefensa con una propuesta regional que nos permita una mayor seguridad en nuestras comunicaciones. No es un secreto que hemos sido objeto de espionajes. Nuestros mandatarios, ciudadanos y funcionarios, que tienen derecho a su privacidad, han sido vulnerados (Aranda, Riquelme & Salinas, 2015, p.111).

En cuanto a los avances, en febrero de 2015 en Uruguay, se firmó entre la Unasur y la Corporación Andina de Fomento (CAF) (Banco de Desarrollo de América Latina) el convenio de "Red de Conectividad Suramericana para la integración" con un aproximado de 1.5 millones de dólares. El proyecto tiene como plazo 30 meses de evaluación para reducir los costos de los precios de los usuarios, lograr el acceso de internet y optimizar la banda ancha (Agencia Pública de Noticias del Ecuador y Suramérica , 2015). Además, la Escuela Suramericana

de Defensa (Esude) con sede en Ecuador comienza sus cursos académicos en 2016 y propone la formación de civiles y militares.

Las iniciativas y propuestas de la Unasur se dirigen a neutralizar la dependencia tecnológica extraterritorial en infraestructura, empresas y Estados, que afirman las vulnerabilidades en relación a las amenazas y operaciones cibernéticas que atentan contra la soberanía de los miembros (Quintero, 2014). Los intereses regionales se han orientado, igualmente, a la capacitación y formación como base para la coherencia conceptual dentro una visión regional. Consecuentemente, existen temas normativos, políticos y metodológicos por definirse ante un escenario internacional que se transforma constantemente.

Este capítulo ha logrado describir la evolución histórica de la seguridad y la defensa en Ecuador desde 1979 a 2016, con el objetivo de contextualizar desde la visión de la seguridad integral la formación de la estructura de la ciberdefensa. La ciberdefensa en Ecuador se ha establecido en materia institucional, jurídica y política; y se ha demostrado un avance, sin embargo, todavía persiste la exclusión de elementos, como aspectos técnicos y regulaciones que afectan la estructura. Así mismo, se ha analizado de manera global el tema de gobernanza de internet, como un elemento relevante en el debate sobre neutralizar amenazas y operaciones cibernéticas. Finalmente, el acercamiento al ámbito regional responde a las directrices de políticas públicas y el compromiso con las iniciativas suramericanas, a la vez, ha permitido definir un escenario de interdependencia regional.

CAPITULO III
ATAQUES CIBERNÉTICOS A INSTITUCIONES ESTATALES, EL CASO SENECYT A TRAVÉS DE LA METODOLOGÍA DE ANÁLISIS Y SU LECTURA DESDE LA GLOBALIZACIÓN, INTERDEPENDENCIA COMPLEJA Y MODERNIDAD LÍQUIDA

3.1. Ciberataques dirigidos a las instituciones del Estado y el caso de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt)

Las revelaciones en 2013, realizadas por Edward Snowden que formaba parte de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), expone la filtración de documentos de inteligencia provenientes de Estados Unidos, que evidenciaron la vulnerabilidad de la privacidad de los ciudadanos, el espionaje a entidades públicas y privadas. Además, expuso la ubicación de centros de inteligencia, particularmente en embajadas (Delgado, 2014). Al respecto, en el panorama internacional se advirtió sobre las nuevas amenazas que se desarrollan en el nuevo espacio relacionado con la cibernética. En el caso de Ecuador, se revelaron ataques cibernéticos de distintos actores y territorios.

Es así, que en 2016 se presentó el caso de la Secretaría de Educación Superior Ciencia y Tecnología (Senescyt) que fue objeto de ataques cibernéticos, y parte de las instituciones que han implementado el Gobierno Electrónico por parte del Estado a través de las TIC, con el objetivo de mejorar de forma cualitativa y cuantitativa los servicios e información que se ofrecen a la ciudadanía (Secretaría Nacional de Planificación y Desarrollo, 2015). Este apartado analiza de manera secuencial los ataques cibernéticos a instituciones del Estado ecuatoriano en el período 2013-2016 y aborda el caso de estudio, en cuanto a la institución, las investigaciones realizadas y el alcance del ciberataque.

3.1.1. Ataques a las instituciones del Estado ecuatoriano

Ecuador en el período del 2011 a 2015, registró diversos ataques a entidades públicas, en los sitios web desfigurados se encuentran entidades pertenecientes a los ámbitos de seguridad, legislativo, cultura, ambiente, transporte, finanzas, entre otros, además, se han detectado vulnerabilidades de las seguridades a servidores que forman parte del sector público (Bravo, 2015).

Adicionalmente, con el objetivo de dimensionar la extensión de los sistemas informáticos, portales existentes y proyectos, en el Anexo 4 se encuentra una matriz detallada de los servicios informáticos de entidades que forman parte de la Administración Pública Institucional y de la función ejecutiva. Los sistemas se formularon y se ejecutaron antes del Plan Nacional de Gobierno Electrónico 2014-2017 (Plan Nacional de Gobierno Electrónico, 2014-2017).

Así, a través del seguimiento y análisis de la prensa y boletines de prensa de las instituciones se encuentran varios casos de ataques a entidades públicas desde 2013 hasta 2016. Comenzando por febrero de 2013, el ministro de Telecomunicaciones Jaime Guerrero informó que el Consejo Nacional Electoral (CNE) detectó un intento de acceso a su sistema informático durante la jornada de elecciones presidenciales. Como resultado, se reveló que existían 1.400 intentos de sabotear el sistema que provenían de un sistema sofisticado de tecnología que ocultaba las direcciones, presuntamente se trataba de un país desarrollado (Agencia Pública de Noticias del Ecuador y Suramérica, 2013). Así mismo, la firma rusa Kaspersky Lab., mencionó que en Ecuador y varios países de América Latina se llevaba a cabo una campaña de ciberespionaje, denominada "Machete". La campaña fue descubierta en 2013 por un general de un país latinoamericano, del cual no se precisó; se mencionó por el experto de seguridad Dmitry Bestuzhev director global de investigación y análisis de Kaspersky Lab., que los atacantes estaban buscando información catalogada como privada y confidencial, de carácter militar, que contenga temas de seguridad nacional de los gobiernos como nóminas, radares y proyectos. Como resultado se detectaron 282 víctimas en Ecuador (El Comercio, 2014).

Para 2014, El presidente de la República Rafael Correa, denunció intentos de filtración de información provenientes de la presidencia y de las Fuerzas Armadas, Comando y Conjunto que tenían como origen presuntamente de Colombia y Estados Unidos. Así mismo, recalcó la importancia de la preparación ante la denominada "guerra cibernética" (El Universo, 2014). En diciembre del mismo año, el operativo "Tempestad" desarticuló la banda que vulneraba los sistemas informáticos de una institución de contratación pública, la banda tenía como objetivo beneficiar empresas y personas naturales en la contratación. El

mecanismo se realizaba mediante un software que borraba las secciones de los usuarios a cambio de dinero (Ministerio el Interior, 2014).

En enero de 2015, se detectó un programa maligno que encriptó archivos sensibles, el ataque estuvo dirigido a 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. La difusión del virus se caracterizó por ser sostenido y masivo. A partir de las primeras infecciones, se tomaron acciones para contrarrestar la amenaza, no obstante, las instituciones perdieron los archivos. Los análisis técnicos de los ordenadores infectados determinaron que el virus se denominaba *cryptolocker*, un malware orientado a los usuarios mediante correos electrónicos con el asunto de "facturación electrónica". Además, los técnicos mencionaron que el malware se difundió debido a la coyuntura existente, pues desde el primero de enero de este año el Servicio de Rentas Internas (SRI) exigió de manera obligatoria la emisión de comprobantes electrónicos a diversas empresas privadas y públicas, que conlleva a la expansión de herramientas electrónicas y por lo tanto, exige reestructurar sistemas y procesos de documentación (Ortega, 2015). Además, en septiembre de 2015, el Ministro Coordinador de Seguridad, César Navas y el Director General de Servicio Nacional de Contratación Pública (SERCOP), Santiago Vásquez, denunciaron el comportamiento inusual del sistema de contratación pública. Contextualizando lo ocurrido, la herramienta realiza transacciones de 10 mil millones de dólares cada año, es decir, el 10% al 15% del PIB, por lo tanto, su buen funcionamiento es fundamental. Como resultado, se reprogramaron 2.500 procedimientos que fueron afectados (Ministerio Coordinador de Seguridad, 2015).

Finalmente, en 2016 se dio a conocer la vulnerabilidad del sistema informático de la Secretaría Nacional de Educación Superior, Ciencia y Tecnología (Senescyt), en el que se registraron títulos de manera ilícita[49].En resumen, los ataques cibernéticos se ejecutaron debido a temas coyunturales o a instituciones que gestionan información y procesos estratégicos, además, como efecto se propagó la prevención sobre el tema a instituciones estratégicas, en especial a las pertenecientes a los sectores financiero, energético, petrolero y

[49] El caso de la Secretaría Nacional de Educación Superior, Ciencia y Tecnología será tratado en la siguiente subsección como caso de estudio.

manufacturero. En efecto, no existen registros sobre los análisis de los ataques cibernéticos a instituciones públicas, sin embargo, la fiscalía ha registrado cifras sobre los delitos informáticos dirigidos a individuos en base a las denuncias y se encuentran detallados en el Anexo 5.

3.1.2. Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

Para comenzar con el análisis del caso de estudio en primera instancia, se establece el contexto institucional. La educación superior ha experimentado diversas transformaciones en su institucionalización, pues las reformas educativas se encuentran vinculadas a proyectos sociales. En este sentido, Ecuador propuso como alternativa estructurar la educación superior desde un carácter público, orientándose al bien común en concordancia con la Constitución y el Plan Nacional del Buen Vivir. (Ramírez, 2013). Las instituciones que se han derivado de esta iniciativa se han enfocado en un modelo tripartito (público, privado y transnacional) (Pilca, 2015). Así, se presenta una breve descripción de la estructura de la educación superior y el Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE).

En concordancia, con la Constitución y la Ley Orgánica de Educación Superior (LOES), el Sistema de Educación Superior se encuentra estructurado por tres instituciones: la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt) (Ver Anexo 3), rectora de la política pública para la educación superior y coordina acciones entre la Función Ejecutiva y las instituciones; el Consejo de Educación Superior (CES), encargado de emitir normas regulatorias, además, sanciona irregularidades y autoriza la apertura de carreras universitarias y el Consejo de Evaluación, Acreditación, y Aseguramiento de la Calidad de la Educación Superior (CEAASES) encargado entre otras funciones, de los temas de evaluación y acreditación de las instituciones y habilitación para el ejercicio profesional (Pacheco & Pacheco, 2015). Los dos últimos son órganos colegiados bajo una composición mixta (Ramírez, 2013).

En cuanto a la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (Senescyt), una vez establecida la delimitación de sus funciones, tiene

como misión, de acuerdo al Estatuto Orgánico de Gestión Organizacional por Procesos (2013), capítulo uno, artículo uno, la rectoría de la política pública en la Educación Superior, la Ciencia, Tecnología, Innovación y los Saberes Ancestrales. Así mismo, es la entidad que vincula el sector público y privado. En esta línea, se han elaborado y ejecutado diferentes propuestas e iniciativas, entre las que se destacan el Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE). El SNIESE, es un servicio de información pública que tiene como objetivo proveer a la ciudadanía información de calidad sobe la educación superior (Secretaria Nacional de Planificación y Desarrollo, 2012). Desde esta perspectiva, se inicia la automatización de la institución.

3.1.3. Sistema Nacional de Información de la Educación Superior del Ecuador y el Operativo "Impacto Inicial"

El sistema SNIESE de la Senescyt se constituye como un espacio público virtual que relaciona a la Secretaría con las instituciones y la ciudadanía. El área de educación superior y la investigación se ha convertido en una prioridad en la agenda del Estado, debido a que se concibe como un bien público pues, aporta al desarrollo y beneficia a la sociedad (Agencia Pública de Noticias del Ecuador y Suramérica , 2015). Adicionalmente, un elemento fundamental es la exigencia y valoración de los títulos en el ámbito laboral. Desde esta perspectiva, resulta evidente la importancia de la información que gestiona y administra el sistema. En este contexto, el operativo "Impacto Inicial" expone el ataque cibernético del sistema de la Senescyt y otras entidades.

Desde el 2010 se inició el proceso de registro de títulos en la Senescyt a través de un sistema informático que, de acuerdo con René Ramírez, secretario de la institución, se evitaba trámites burocráticos que anteriormente se realizaban de forma manual (Ministerio del Interior, 2016). En el caso del registro de títulos nacionales, se encargan de ingresar las instituciones de educación superior al SNIESE. Así, el registro de títulos son responsabilidad de la institución de educación superior dentro del plazo de 30 días a partir de la fecha de graduación, de este modo, el graduado no realiza ningún trámite (Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación, s.f.). Específicamente,

cada institución posee un código que utilizan a través de las secretarías para registrar a cada estudiante graduado que, a su vez tiene un código propio de asignación. El filtro que realizaba en ese momento la Senescyt era verificar la validez de los códigos mediante algoritmos informáticos, mas no el detalle de cada título debido a la cantidad de información (Zamora, 2017). Por otro lado, el registro de títulos universitarios extranjeros se realiza mediante el trámite directamente del graduado (Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación, s.f.).

Al respecto, el operativo "Impacto Inicial" se presenta como un trabajo en conjunto de la Fiscalía y el Ministerio del Interior, con el fin de investigar sistemas informáticos vulnerados. El inicio de las investigaciones por parte de la Fiscalía comenzó en octubre de 2015, con una duración de cuatro meses y, por parte del Ministerio del interior, tuvo una duración de ocho meses. En efecto, se determinó la presencia de una red *hackers* que habrían vulnerado el sistema de entidades bancarias y públicas que operaban en el país. El operativo surge debido a las denuncias realizadas por parte de las autoridades y técnicos de la Senescyt y la ANT (Ministerio del Interior, 2016).

El 8 de enero de 2016, la Policía Nacional a través de la Dirección de Inteligencia y su Unidad de Inteligencia, Contrainteligencia y Coordinación Transnacional (DGI-Uicct), desintegró la red internacional de *hackers*, en conjunto, con la coordinación de la Fiscalía. El operativo consistió en nueve allanamientos simultáneos desplegados en las provincias de Pichincha, Guayas, Santo Domingo de los Tsáchilas e Imbabura (Ministerio del Interior, 2016). En la ciudad de Quito, los allanamientos y detenciones se realizaron en los sectores de Nayón, Ponciano, San Juan y El Inca. Por otro lado, en la ciudad de Guayaquil, se realizaron en los sectores de Tarqui, La Garzota y La Puntilla (Expreso , 2016).

Finalmente, los detalles de la operación se revelaron el 16 de enero de 2016 mediante una rueda de prensa presidida por José Serrano, ministro del Interior, René Ramírez, secretario de Educación Superior Ciencia, Tecnología e Innovación (Senescyt) y Lorena Bravo, directora ejecutiva de la Agencia Nacional de Tránsito (ANT). Los resultados obtenidos de la investigación demostraron que

la organización criminal vulneraba los sistemas de las dos instituciones (Ministerio del Interior, 2016). El operativo evidenció la necesidad de estructurar la defensa y seguridad de los sistemas que gestionan las instituciones.

3.1.4. Alcance del ataque cibernético: Resultados de las investigaciones[50]

En general, los resultados de las investigaciones a partir de la rueda de prensa se difundieron en boletines de las entidades que participaron en el operativo y en la prensa. Para comenzar, la banda de hackers operó aproximadamente 18 meses, tiempo en que movió alrededor de un millón de dólares (Ortiz, 2016). Es así, que el ocho de enero se detuvieron a diez personas, uno de nacionalidad colombiana y un servidor público perteneciente a la ANT. Dentro de las evidencias se encontraron sellos del Ministerio de Educación, papeletas con depósito de montos superiores al millón de dólares, cheques de diversas entidades bancarias, dinero en efectivo, varios documentos, dispositivos electrónicos como celulares y computadoras portátiles, entre otros (Ministerio del Interior, 2016).

En el caso de la Senescyt, se evidenció el registro ilegal de 366 títulos falsos de los 1.620.00 registrados, en los que la mayoría de los títulos se presentaban de cuarto nivel, es decir, maestrías y doctorados. Entre los resultados de las investigaciones, se identificó que pagaban entre USD $ 1.000 y US $ 10.000 por el proceso de registro (Agencia Pública de Noticias del Ecuador y Suramérica , 2016). Adicionalmente, con la información entregada de la Fiscalía, los títulos se dividían en diferentes áreas: Derecho con el 40,6%; Educación comercial y administración con el 35,9%; informática con el 6,3%; Ciencias de la Educación con el 3,1% y Medicina con aproximadamente el 2%, se encuentran representados gráficamente en el Anexo 6 (Agencia Pública de Noticias del Ecuador y Suramérica , 2016).

Por su lado, la Secretaría Nacional de Administración Pública (SNAP) que también controla y vigila el proceso del gobierno electrónico, solicitó al Ministerio del Trabajo el listado de las personas que se encontraban laborando en el sector

[50] Hasta marzo de 2016 cuatro de los diez procesados en el caso recibieron dos años de prisión, después de aceptar su participación por el delito de asociación ilícita (La Hora, 2016).

público. En este caso, la SNAP recibió por parte de la Fiscalía dos listas: la primera con 81 nombres y la segunda con 285, correspondientes a las dos etapas de la investigación. En la nómina entregada constan los datos completos, la universidad y la profesión que ejercían. Así, el informe por parte del Ministerio de Trabajo sería el sustento legal para que la SNAP proceda con acciones administrativas en contra de los responsables, como la desvinculación, la imposibilidad del reingreso y el no pago de la indemnización (Ortiz, 2016).

Dentro del listado de las personas que obtuvieron el título de abogado ilícitamente, se remitió la lista al Consejo de la Judicatura para determinar si participaron en causa o ejercen cargos en el sistema judicial. En concordancia con el fiscal general del Estado, Galo Chiriboga, en ese caso se invalida los procesos y se declararan nulos, conjuntamente, se iniciaría un proceso penal por ejercer la profesión sin validez (Agencia Pública de Noticias del Ecuador y Suramérica , 2016). En efecto, las sanciones se extenderían a la responsabilidad penal, por adquirir servicios de una red delictiva de *hackers* (Ortiz, 2016). Entre las diversas personas que se encontraban en la lista, se destacó el nombre de Lucía Valecilla, abogada de Luis Chiriboga, en ese momento, presidente suspendido de la Ecuafútbol (Jácome, 2016). El nombre de la abogada, contribuyó a que el caso sea de interés público y según Byron Zamora[51] (2017) a que el caso tengo un alcance mediático amplio desde lo político, social y jurídico.

En el ámbito legal, el día 9 de enero se formularon cargos por asociación ilícita de los detenidos por el Fiscal Diego Correa en la Unidad de Flagrancia de Pichincha. La Fiscalía presentó el informe de seguimiento y vigilancia, intercepción de llamadas telefónicas, informe de inspección ocular técnica y pruebas que se incautaron el día del allanamiento. Por lo tanto, Luz Serrano Lasso, jueza de la Unidad de Garantías, dictó prisión preventiva de los diez ciudadanos (La Hora, 2016). La instrucción fiscal tiene una duración de 90 días, desde la fecha en la que se mantuvo la audiencia de formulación de cargos (Ecuadorinmediato, 2016). El caso de asociación ilícita se encuentra normada en el COIP en el artículo 370 que establece que:

[51] Byron Zamora trabajó en la Senescyt en el período 2013-2016 como Director Subrogante de Comunicación y Comunicador Social.

> Cuando dos o más personas se asocien con el fin de cometer delitos, sancionados con pena privativa de libertad de menos de cinco años, cada una de ellas será sancionada, por el solo hecho de la asociación con pena privativa de libertad de tres a cinco años (COIP, 2014, art. 370).

Finalmente, el operativo evitó la realización de las transferencias ilícitas y se determinó que la organización tenía como objetivo vulnerar el sistema del Banco Central del Ecuador, para intervenir y cambiar el estado de cuentas congeladas y decomisadas, se trataba de dinero que se iba a transferir a entidades bancarias en la República de Colombia (Ministerio del Interior, 2016). Para Andrés Delgado (2017), el ciberdelito se categoriza en un nivel de amenaza bajo debido a que no se perdió la base de datos original del SNIESE, sino se agregaron datos de las personas que a través de una comparación entre bases de datos de las instituciones de educación superior y la SNIESE, se reconoce quien contrajo los servicios de registro ilícito de títulos. El ataque cibernético tuvo un efecto en diversas entidades y en la opinión de la ciudadanía sobre la efectividad de los sistemas de seguridad y defensa de las instituciones estatales. Es así, que se considera que la vulneración de los sistemas y la gestión de la información incurren en las amenazas a la que se encuentran expuestas las entidades del sector público.

3.2. El agente de amenaza, el objetivo y el seguimiento institucional

El alcance y el impacto de las TIC en el ámbito de administración, gestión y gobierno del sector público, se ha consolidado como un proceso democrático que permite la interacción entre distintos actores de la sociedad. Sin embargo, el desarrollo y la implementación también supone desafíos como la construcción de condiciones jurídicas, técnicas y barreras culturales (Vargas, 2011). Si bien lo anterior recoge algunos de los inconvenientes que se presentan como parte de trasladar información y datos al ciberespacio, también es importante reconocer que en este dominio existen amenazas y vulnerabilidades que tienen consecuencias en la conducción de las instituciones y el bienestar del Estado.

Así, este apartado se centra en el estudio de los objetivos de los ataques cibernéticos en el sector público, resultado de la investigación del Centro Criptológico Nacional- CERT de España en el año 2016; y el análisis institucional en base a la metodología propuesta por Choucri, Madnick y Koepe (2016), quienes enfocan su investigación en el censo de instituciones en el ciberespacio[52].

3.2.1. Los objetivos de los ataques cibernéticos en las entidades públicas

La modernización y automatización del sector público con el objetivo de mejorar los servicios ha estructurado el empleo y la utilización de instrumentos de las TIC que faciliten y agilicen los procesos burocráticos, enfocándose en el cumplimiento de los derechos de la ciudadanía. Así, el sector público se ha expuesto a ataques cibernéticos públicos o anónimos que se dirigen a instituciones del Estado y que tienen un impacto en la sociedad y el gobierno, pues, afectan distintos sectores de un país como las infraestructuras críticas. De esta manera, es importante determinar los objetivos de los ataques en el sector público.

A pesar de los sistemas de ciberdefensa y ciberseguridad de los Estados, existen ataques cibernéticos que demuestran las vulnerabilidades presentes. La tabla 4 establece un criterio de clasificación de los ataques cibernéticos en el sector público en base a las amenazas más representativas durante el año 2016. En el gráfico 1 en la subsección titulada "El nuevo campo de batalla: actores y operaciones cibernéticas" ya delimita el grado de daño y el grado de organización del actor que realiza el ataque, no obstante, la tabla detalla y amplía los agentes de amenaza y específica los objetivos de los ataques en el sector público.

[52] Posteriormente, se analizará el caso de la vulnerabilidad del SNIESE en el capítulo IV, en base a la recopilación de información.

TABLA 4

OBJETIVOS DE LOS ATAQUES CIBERNÉTICOS DIRIGIDOS AL SECTOR PÚBLICO

Agentes de las amenazas	Sector Público
Estados	Ciberespionaje político
	Cibercapacidades ofensivas
Organizaciones Criminales	Robo y publicación o venta de información
	Manipulación de la información
	Disrupción de sistemas
	Toma de control de sistemas
Ciberterroristas	Disrupción de sistemas / toma de control de sistemas
Ciberactivismo	Robo y publicación de información
	Desfiguraciones
	Disrupción de sistemas
	Toma de control de sistemas
Cibervándalos y script-kiddies	Robo de información
	Disrupción de sistemas
Actores Internos	Robo y publicación o venta de información
	Disrupción de sistemas
Ciberinvestigadores	Publicación de información

Código de colores		
Bajo	**Medio**	**Alto**
No se han observado nuevas amenazas o tendencias, o	Se han observado nuevas amenazas o tendencias, o	Las amenazas o su tendencia se han incrementado significativamente.
Se dispone de medidas suficientes para neutralizar la amenaza, o	Se dispone de medidas (parciales) para neutralizar la amenaza, o	Las medidas adoptadas tienen un efecto muy limitado, por lo que la amenaza permanece.
No ha habido incidentes especialmente significativos en el periodo analizado.	Los incidentes detectados no han sido especialmente significativos.	Los incidentes detectados han sido especialmente significativos.

Fuente: Criptológico Nacional (CCN-CERT), 2016
Elaborado por: Criptológico Nacional (CCN-CERT) (2016)

En este sentido, se encuentran factores a considerar en el alcance de los objetivos como el origen, motivación y nivel de conocimiento de los ataques o

amenazas. En cuanto a las motivaciones, se relación directamente con el agente, se presentan desde mejorar la posición geopolítica o estratégica, protección de seguridad nacional, beneficio económico, objetivos ideológicos, influir en decisiones políticas, búsqueda de desafíos, venganza, revelación, etc. En el cuadro del código de colores se delimita también el nivel de conocimiento, en el que se especifican como bajo, medio y alto en correlación con los factores descritos (Centro Criptológico Nacional- CERT, 2016).

Dentro de los criterios presentados en la tabla 4 se destaca la información como un elemento fundamental, pues se encuentra como prioridad en el desarrollo de los derechos fundamentales reunidos en los textos de Declaraciones Universales, constituciones y normativas de los Estados democráticos, así, exige que los sistemas de información se encuentren permanentemente operativos (Galán & Cordero, 2016). Es así, que existe mayor disponibilidad de información estratégica a todos los niveles de la sociedad, por lo tanto, se considera una cuestión nacional. La capacidad de controlar el acceso, los sistemas y todos los recursos de la información se presenta como una prioridad en las estrategias de ciberdefensa y ciberseguridad. La información estatal y sus componentes se conciben como la base sobre la cual se establecen líneas de actuación.

Según Mathew Gyde del Group Executive-Security de Dimension Data (2017), establece que los gobiernos se encuentran en constante amenaza y ataque debido a que las instituciones gestionan amplías cantidades de información sensible, por ejemplo: perfil de los servidores, presupuestos, comunicaciones, investigaciones de inteligencia, planes de desarrollo, negociaciones, proyectos debates, etc. (Rozalén, 2017). De esta manera, resulta primordial la conducción de cibercapacidades para la seguridad y defensa de las instituciones de los Estados en base a las tendencias y conocimientos que se generan a raíz de las tecnologías emergentes.

3.2.2. Seguimiento institucional: metodología

En el panorama propuesto los ciberataques se convierten en una amenaza constante. De este modo, en la tabla 4 se logra identificar los actores y acciones

que forman parte de las amenazas a los sistemas cibernéticos del Estado. Considerado la complejidad del ciberespacio en cuanto a su ubicuidad, escala y alcance es necesario determinar y representar las instituciones que responden ante los cambios constantes del escenario nacional e internacional, tanto en el ámbito real como virtual. Debido a incidentes cibernéticos en diferentes escalas, los gobiernos analizan las posibilidades de potencializar sus capacidades frente a las amenazas emergentes. En respuesta, los gobiernos movilizan recursos nacionales e internacionales para la creación de un marco de seguridad y defensa cibernética (Choucri, Madnick, & Koepe, 2016).

Para Choucri, Madnick y Koepe (2016) el análisis del contexto teórico de las instituciones en el dominio cibernético mantiene una dinámica inversa a la literatura tradicional, es decir, las instituciones pueden ser las precursoras de formalizar normas y principios que, a su vez, podrían consolidar y fortalecer las propias instituciones. Mientras que se tiende a argumentar que el consenso de normas precede a la formación de las instituciones. Adicionalmente, los autores mencionan que las organizaciones que se desarrollan en torno al ciberespacio no tienen mandatos claros y tienen una superposición de esferas de influencia.

La metodología propuesta por Choucri, Madnick y Koepe (2016) tiene como objetivo destacar entidades, señalar sus relaciones e interconexiones y compilar un censo de instituciones. Como objetivo secundario, se explora la calidad de los datos y se infiere el desempeño organizacional. Los criterios que se utilizan se dividen en: a) suministro de datos cualitativos y cuantitativos públicos del área de interés (internacional, nacional, intergubernamental, sin fines de lucro y el sector privado) y, b) la responsabilidad de la coordinación basada en mandatos formales emitidos por los organismos. En el análisis realizado los autores se enfocan en establecer un "ecosistema institucional" del sistema de ciberseguridad.

La tabla que presentan los autores recoge tres elementos. Primero, se determina el rol que cumple la institución. Segundo, se analiza la disponibilidad de datos que se clasifican en tres niveles: bajo, moderado y alto, que depende de las variables que presenta cada entidad. Tercero, los ejemplos de las variables se encuentran desde datos métricos, estadísticos, encuestas, datos secundarios de

conferencias, alertas, reportes, publicaciones entre otros documentos relacionados con ciberseguridad y ciberdefensa, cabe mencionar que existen entidades que tienen información clasificada como confidencial.

Igualmente, realizan un análisis de la estructura organizacional, la coordinación con otras organizaciones y suministro de datos. Las instituciones más representativas presentadas en el análisis son el Computer Emergency Response Team (CERT), Information Sharing Analysis Center (ISACs), Information Sharing and Analysis Organizations (ISAOs), respuestas Intergubernamentales, entre otras. En efecto, establecen que las diversas instituciones existentes tienen diferentes misiones, mandatos, intereses y restricciones. Finalmente, la evidencia sugiere que existe poca coordinación institucional, que representa el grado de desconexión y la cambiante dinámica de las amenazas (Choucri, Madnick, & Koepe, 2016).

3.3. Globalización, interdependencia compleja y modernidad líquida

La estructura del sistema internacional se caracteriza por tener Estados y sociedades conectadas a través de las TIC, es así, que el origen de un nuevo dominio como el ciberespacio ha cambiado las dinámicas de los actores. Debido a la magnitud de los elementos que se encuentran, es necesario delimitar la lectura, de esta manera, se utilizan para el análisis desde el ámbito de las relaciones internacionales, las teorías de la Globalización, la Interdependencia Compleja y la Modernidad Líquida. La expansión de la tecnología y de los diversos canales de comunicación se han fundamentado en la globalización, que ha provocado un mayor grado de interdependencia entre los Estados. La complejidad de estas relaciones se puede explicar a través de la interdependencia compleja, sin embargo, debido a la naturaleza del ciberespacio, factores como el accionar de individuos y amenazas fluctuantes, se recurre a la modernidad líquida.

El presente subcapítulo pretender desarrollar algunos conceptos clave de las teorías propuestas, que se vinculan con temas desarrollados a lo largo de la investigación, la estructura de la ciberdefensa en Ecuador y en efecto, se enlaza al caso y el resultado del análisis metodológico de la vulnerabilidad del SNIESE.

3.3.1. El rol de la globalización en el desarrollo del ciberespacio

La convergencia de las comunicaciones y la dinámica tecnológica ha tenido un efecto en el panorama internacional y, en el caso de los Estados ha influenciado en la adopción de estrategias en todos los niveles que conforman. El proceso globalizador resultado del desarrollo de las TIC ha configurado una transformación de la sociedad mundial en todos los sectores, así, se ha establecido el ciberespacio, la ciberdefensa y la ciberseguridad, además de las operaciones cibernéticas que se han descrito a lo largo de la investigación. En este escenario, el rol de la globalización permite explicar los componentes que se presentan alrededor de estos conceptos.

De acuerdo con Göra Therborn, la tendencia globalizante comprendida como "aceleración o intensificación de grandes procesos sociales de alcance e impacto, al menos, de nivel continental" (Molina, 2014, p.3), ha estado presente en las olas históricas. Para Osterhammel y Peterson (2005), la última ola se ha reconocido como la "globalización", el alcance conceptual se desarrolla a finales de los ochenta. Como resultado, ha modificado el tiempo y el espacio, también, las conexiones y canales de comunicación se han expandido en un cambio acelerado, a través de dispositivos cibernéticos (Molina, 2014). De este modo, el ciberespacio y demás conceptos, son combinaciones de distintas dimensiones que se conforman por diversos actores.

Desde este panorama, la interacción entre los diferentes actores es de carácter internacional y se desenvuelve en una red de interacciones. Así la situación, en concordancia con Beck (2004)

> el Estado se convierte en uno más de los actores políticos planetarios y pierde protagonismo, ahora compite o colabora con una nueva constelación de actores políticos a escala global, que invaden a menudo el ámbito de decisiones que el Estado había considerado como propio y exclusivo (Beck, 2004, p.33).

Desde esta visión, el Estado todavía permanece como ente principal en la toma de decisiones, sin embargo, la globalización ha influenciado para que la proliferación de nuevas entidades limite su autonomía y, gradualmente su soberanía (Restrepo, 2013).

Bajo ese orden de ideas, las instituciones pertenecientes a los Estados han experimentado el surgimiento de actores que afectan su comportamiento y su desempeño. En torno a las consideraciones anteriores, el ciberespacio constituye un dominio que alberga datos e información y, por otro lado, se considera el espacio en el que se presenta la aparición de las operaciones cibernéticas, que han crecido y se han consolidado como amenazas a la nación en todos sus niveles. En efecto, la globalización ha acelerado el proceso a través de las TIC y la madurez tecnológica que cambia constantemente y produce efectos en la estructura estatal.

Desde esta perspectiva, los ataques cibernéticos realizados a entidades públicas de Ecuador han vulnerado sus capacidades para su eficaz desempeño. En temas coyunturales, se han identificado ataques cibernéticos que provienen de distintos países e incluso campañas de ciberespionaje como "Machete" que se dirigen a nivel regional. Adicionalmente, existen programas que se expanden a nivel mundial, mediante las TIC y que afectan a las instituciones y personajes públicos. La globalización abarca varios actores que progresivamente, por un lado, pueden ser alcanzados por los ataques y, por otro lado, forman parte de los atacantes.

En el caso Senescyt, se analiza desde una visión global a pesar que la vulnerabilidad del sistema se realizó dentro del territorio. Sin embargo, existía la vinculación con otro Estado. Los sistemas informáticos se encuentran conectados a través de redes que permiten que la información se desplace de un territorio a otro. Por otra parte, las intenciones de la red de *hackers* de transferir dinero a entidades bancarias en Colombia se presentan como una situación común en estos temas, pues la organización criminal en este dominio tenía la capacidad de gestionar capital desde las instituciones de Ecuador hacia Colombia. La accesibilidad a la tecnología abrió este espacio y sus efectos a las actividades humanas. Entonces, el Estado se encuentra inmerso en desarrollar elementos

jurídicos, políticos y técnicos que avancen acorde a la constante evolución que conlleva la globalización, en especial en las dinámicas transfronterizas, así, resulta importante la cooperación con instituciones internacionales, que no se registra en el caso.

3.3.2. Interdependencia compleja y el nuevo canal de conexión

La globalización ha originado un contexto internacional en que los actores se encuentran difícilmente desconectados los unos de los otros. Desde el enfoque de Robert O. Keohane y Joseph S. Nye (1989, p.165) se conoce como interdependencia, y lo autores la definen como "la ausencia del uso de la fuerza, la falta de jerarquía en los asuntos a tratar y la presencia de múltiples canales de contacto entre las sociedades". El concepto de la interdependencia se presenta en las relaciones internacionales en un escenario complejo, donde los actores toman las decisiones en base a un engranaje mundial establecido y donde existe la necesidad de recursos que los obliga a limitar su soberanía y autonomía (Rivera, 2004). Entonces, analizando el concepto se encuentran tres elementos fundamentales: la ausencia de la fuerza, la falta de jerarquía en los asuntos a tratar y múltiples canales de contacto.

Para comenzar, la agenda internacional se ha expandido a un cúmulo de temas que ya no se centran en los tradicionales como la seguridad militar (Keohane & Nye, 1989). Los tópicos se extienden desde ecológicos, culturales, tecnológicos, económicos, etc., y la interacción entre Estados no tiene una jerarquía establecida (Rivera, 2004). Ahora bien, los gobiernos ante la interdependencia no utilizan la fuerza militar para resolver conflictos económicos y sociales. Por lo tanto, los Estados se adaptan a nuevas políticas que reflejen el bienestar común (Murillo, 2013). En este sentido, el uso de la fuerza ya no prima en las agendas de diversos Estados debido a la importancia en la que se centran otros temas, como el ciberespacio y las temáticas que se derivan. Los problemas que provienen de este concepto ya no se consideran de índole doméstico, sino traspasan fronteras y, las instituciones son las encargadas de coordinar soluciones, éstas reflejan la identidad, valores políticos de la población y de cada país (Keohane, 1998).

Desde la misma línea de pensamiento, existen dos conceptos: sensibilidad y vulnerabilidad. El primero se refiere al nivel de respuesta dentro de una estructura definida, es decir, a los cambios y costos que generan las interacciones y, asume que ante estos acontecimientos se persistirá sin cambios. Por otra parte, la vulnerabilidad experimenta costos impuestos por hecho externos, se da en un marco de modificaciones con el objetivo de cambiar la situación. En esta apreciación, se puede distinguir que el primer concepto refleja la dificultad de modificar, en cuanto al segundo incluye la dimensión estratégica (Rivera, 2004).

Para Keohane y Nye la interdependencia compleja se determina por múltiples canales que conectan diversos actores de la esfera internacional, así, pueden ser interestatales, transnacionales e intergubernamentales. En efecto, se direccionan las interacciones que resultan de las relaciones y las políticas internacionales (Prieto, 2011). Es así, que en estos múltiples canales se encuentra el ciberespacio, como un canal que genera vínculos entre los actores, que cumplen un rol y que influyen en los escenarios internos como externo de los Estados, pues las actividades que realizan interfieren en los intereses de los países. Por lo tanto, debido a su alcance origina una situación de interdependencia en el dominio virtual.

La lectura se analiza en el mismo orden de ideas. A través del análisis histórico de Ecuador, se evidencia que ha reestructurado su agenda y su discurso a temas relacionados con el Buen Vivir y la seguridad integral, que ha direccionado a las temáticas de la ciberdefensa y la ciberseguridad. A pesar del enfoque constructivista del Estado ecuatoriano, el sistema internacional en cuanto al ciberespacio se encuentra con Estados dependientes en materia de infraestructura, redes y tecnología. Por lo tanto, el actuar del Estado es limitado y su autonomía es afectada por estructuras y dominio de diversos elementos que forman parte de este dominio.

Así mismo, con el surgimiento de diversos actores se ha requerido un enfoque que comprenda necesidades en seguridad y defensa en el ámbito local e internacional, sin embargo, la política de un Estado no tiene un alcance global y responder a las operaciones y amenazas cibernéticas se convierte en un tema

complejo. Es así, que se presentan las vulnerabilidades y se centran en el tema jurídico, institucional y técnico. La escasez de herramientas y elementos fundamentales como infraestructura y conocimiento tecnológico son una desventaja. Desde este argumento, las cuatro instituciones que forman parte del caso se han direccionado desde un nivel moderado y bajo en la investigación, sin embargo, en el momento no existió prevención, que sería parte del rol del Comando de Ciberdefensa, que fue creado paralelamente al ataque cibernético. Esta situación percibe costos, como recursos en investigación y, a pesar de modificar leyes, políticas e instituciones, la constante innovación de las operaciones cibernéticas representa desafíos en cuestión de seguridad y defensa.

Finalmente, la tecnología y la comunicación se han convertido en factores que conectan los diferentes actores del escenario internacional, así, las relaciones interdependientes, también comprenden la disminución de autonomía. En este sentido, en un entorno donde existen actores "no territoriales" que se han empoderado en el panorama internacional, las vulnerabilidades de los Estados se hacen evidentes como en el caso de la Senescyt, y las agendas se han centrado en establecer asuntos prioritarios en cuanto a seguridad y defensa cibernética.

3.3.3. La metáfora líquida: la fluctuación de nuevos actores y amenazas

La interdependencia compleja permite explicar el sistema internacional, no obstante, en el "ciberespacio" como canal de comunicación, se extiende y se aproxima a los individuos como actores que trascienden y se encuentran en constante estímulo con la tecnología, que permite su fluidez continua y flexibilidad en este nuevo dominio, como efecto genera incertidumbre y desconocimiento de nuevos atacantes y se conforman relaciones más complejas. En este caso, los fenómenos del ciberespacio, ciberdefensa y ciberseguridad se analizan desde la desde la perspectiva de la modernidad líquida, debido a la transitoriedad de las nuevas formas de operaciones y relaciones cibernéticas. Así, la teoría de la Modernidad Líquida se propone como una metáfora de Zygmunt Bauman, que demuestra la transformación de los órdenes sociales y la "licuefacción" de las estructuras consolidadas. La discusión se desarrolla en torno a las características de los líquidos y los sólidos.

Bauman utiliza la figura de la "liquidez" para describir el mundo contemporáneo. De esta manera, para el autor, la tesis fundamental se basa en la transición de una modernidad sólida a una líquida en el que las estructuras sociales no son perdurables y se figuran de transformación y transitoriedad, y la sociedad líquida es cambiante e impredecible. Por lo tanto, la modernidad líquida se concibe en un tiempo de incertidumbre, que responde a las transformaciones del sistema de seguridad que protegían al individuo (Vásquez, 2008). El análisis, se enfoca en las cualidades de los líquidos. La característica principal es que "los fluidos, por así decirlo, no se fija al espacio ni se atan al tiempo" (Bauman, 2002, p.8), así, entre la relación tiempo-espacio, se considera que para los líquidos el espacio es fundamental, puesto que pueden dominarlo por instantes limitados, para luego seguir fluyendo. Además, la velocidad que recorre depende de la tecnología, que a través de recursos e ingenio se logra aumentar la distancia recorrida por una unidad de tiempo, es así que el tiempo conquista el espacio (Bauman, 2002).

Por otra parte, el autor introduce el sistema de vigilancia del "panóptico" de Michel Foucault en base a Jeremy Bentham, que propone como una metáfora del poder moderno. El sistema se basa en la visibilidad que tiene el vigilante sin el conocimiento de los internos que se encuentran inmovilizados y confinados, mediante límites y rutinas. Además, se debe mencionar que el análisis se realiza también en el primer capítulo a través de Ofelia Tejerina y se propone también el concepto de "banóptico". No obstante, para Bauman, el objetivo es establecer la vinculación existente que se posee sobre el tiempo. Por lo tanto, considera que el tiempo es el secreto del poder y, la técnica del poder se establece en la capacidad de evasión (Bauman, 2002). Es importante mencionar que en literatura posterior Zygmunt Bauman en conjunto con David Lyon (2013) analizan el "post-panóptico", pues han aparecido nuevas formas de control alejadas del encarcelamiento, que con frecuencia también comparten características de flexibilidad y diversión vinculados al entretenimiento y al consumo (Bauman & Lyon, 2013).

En la misma línea de pensamiento, la tesis líquida de Zygmunt Bauman analiza la "vigilancia", que incluye a la tecnología en servicio de la vigilancia. En

el contexto, en el que se encuentra una saturación de dispositivos de vigilancia, Bauman propone una nueva paradoja, "por un lado estamos más protegidos que cualquier generación anterior, y por el otro lado ninguna generación anterior experimentó como la nuestra la sensación cotidiana de inseguridad" (Bauman & Lyon, 2013, p. 112-113). La sociedad se caracteriza por ser adictiva a la seguridad, además, menciona que "todos necesitamos designar a los enemigos de la seguridad para evitar ser considerados parte de ellos" (Bauman & Lyon, 2013, p. 11).

La primera propuesta de la Modernidad Líquida en relación a las características de los líquidos, se asocian a nuevos actores en el ciberespacio que, a través de este dominio fluyen con ayuda de la tecnología por diferentes espacios dentro y fuera del territorio de donde se encuentran. En este sentido, red de *hackers* y organizaciones criminales con el conocimiento tecnológico adecuado pueden invadir espacios públicos, como lo ocurrido al SNIESE. Si bien Ecuador ha establecido un aparataje en pro de la ciberdefensa y ciberseguridad no ha respondido a la protección de información estatal, incluso ante ataques cibernéticos de bajo riesgo, sino se ha centrado en la vigilancia de distintas operaciones de la sociedad civil, a través de sistemas de vigilancia como ECU-911 que responden a la lógica del "panóptico", recopilación de datos y automatización de los servicios públicos.

La magnitud de la expansión de la tecnología y con ella datos e información, la ciberseguridad y la ciberdefensa se imponen en la agenda de internacional y local. La aparición de actores que amenazan a la seguridad estatal, que fluyen en el ciberespacio promueven el temor y son fuente de incertidumbre. La vigilancia se ha estructurado en aras de la seguridad ciudadana, no obstante, a nivel estatal se experimenta vulnerabilidades de instituciones estratégicas como las de Educación Superior y los esfuerzos se perciben como irrelevantes para responder a las necesidades de seguridad y defensa en este nuevo dominio.

El presente capítulo se centró en presentar los ataques cibernéticos que han ocurrido en el período 2013-2016 en Ecuador y se expuso el caso de estudio sobre la vulnerabilidad del sistema SNIESE de la Senescyt, correspondiente al último

trimestre del 2015 e inicio del 2016. Así mismo, se determinó los objetivos de los agentes de amenaza en el sector público, y se enfocó en la importancia de la información estatal. A través de la metodología de análisis institucional, se permite la clasificación de instituciones que intervinieren y participan en el ciberespacio, con el objetivo de relacionar la estructura originada por el sistema internacional y los Estados en relación a la ciberdefensa y ciberseguridad. Desde esta perspectiva, se realizó un acercamiento a las teorías desde el rol de la globalización, la Interdependencia Compleja y la Modernidad Líquida.

VI. ANÁLISIS

En el desarrollo de la disertación se ha estudiado la vulnerabilidad del Sistema Nacional de Información de la Educación Superior del Ecuador en el marco de la estructura de la seguridad integral y la ciberdefensa. Este acercamiento ha permitido afirmar el objetivo general propuesto de analizar la vulnerabilidad de la seguridad informática ante las nuevas tecnologías y sus efectos colaterales en el periodo 2013-2016. Por lo anterior, se profundizarán tres aspectos. En primera instancia, se establece un examen analítico-conceptual de la seguridad integral desde la perspectiva de Ecuador, relacionado con el accionar del Estado en la configuración de instituciones y toma de decisiones. En segunda instancia, se presenta el estado de arte de la ciberdefensa para contextualizar el desarrollo de la institucionalidad, el marco legal y las políticas plasmadas en pro de la defensa cibernética del aparataje estatal. En tercera instancia, se efectúa una descripción lineal de los ataques cibernéticos y se analizan los hallazgos de las metodologías empleadas al caso de estudio. Dentro de lo anterior y a lo largo del análisis, se realiza el alcance de las teorías interdependencia compleja y modernidad líquida.

Posterior a los ataques al Sistema Nacional de Información de la Educación Superior del Ecuador, que se produjeron dentro de un operativo, se evidencia que existían y podían extenderse a las diferentes entidades públicas. En este contexto, establecer los autores que realizaban las operaciones ilícitas en un dominio virtual resultaba difícil y ambiguo. No obstante, las instituciones que intervinieron en la investigación definieron quiénes realizaban el proceso de registrar títulos de forma ilícita y se revelaron los detalles de los resultados de las indagaciones. Por ello, definir conceptos de seguridad es fundamental para proteger la condición, los sistemas y la información estatal. En el caso de Ecuador, la concepción de la seguridad integral abre la posibilidad de nuevas amenazas y lógicas que afectan el comportamiento del Estado.

Ecuador desde el 2008 establece la seguridad integral como referente en el desarrollo de políticas, leyes e instituciones. La perspectiva de seguridad integral se concibe desde un discurso constructivista del Estado ecuatoriano, pues se

fundamenta en el desarrollo humano y el equilibrio de su entorno, así, se encuentra cargado de ideologías desde una visión latinoamericana. El concepto al abarcar diversas temáticas, se acerca a la definición de "securitización". Siguiendo a Buzan (1998), es el discurso de elevar cualquier tema a un "problema de seguridad" es intersubjetivo y otorga legitimidad general y el poder de definir el objeto y la percepción de amenaza. Así mismo, la seguridad integral se presenta como un concepto discursivo que, al proteger los diversos niveles del ser humano y el Estado, su limitación se presenta en los recursos del gobierno y de las instituciones. En este sentido, si se añade el vector del ciberespacio la creación de la estructura para proteger los diferentes niveles que menciona la seguridad integral comprende nuevos costos y conocimientos.

Ahora bien, más allá del discurso constructivista de la seguridad integral, el sistema internacional se ha establecido entorno a un orden mundial que incluye diferentes dinámicas de los actores y condiciona a los Estados en lo que mencionan Keohane y Nye, la interdependencia compleja. La intensidad de la interdependencia, se refleja en la estructura del ciberespacio que se ha originado, de acuerdo a Kuehl (2014), a través de las TIC que configuran redes interdependientes e interconectas. De esta manera, el Estado y sus diferentes entidades deben afrontar la seguridad de su aparataje, es ahí que, desde la perspectiva de la interdependencia compleja, se añade a la agenda el tema del ciberespacio. El Estado ha tenido que direccionar sus esfuerzos a un nuevo concepto que surge como un nuevo canal de conexión entre los Estados en un escenario internacional globalizado. Debido a ser un concepto abstracto, la complejidad que presenta supone un desafío en la comprensión de la magnitud de su alcance y dominio. La influencia estratégica obligó a Ecuador a acercarse a esta concepción, en especial por las amenazas en las redes, pues se presentaron entre los años 2013 y 2016 en base al seguimiento de la prensa y boletines de prensa seis casos representativos de ciberataques, sin mencionar que existen casos que no se encuentran socializados ni registrados.

Los eventos anteriormente nombrados, contribuyen a que el Estado ecuatoriano minimice los conflictos que surgen de este dominio. Este análisis nos dirige a la ciberdefensa. La ciberdefensa con la dispersión terminológica ha

limitado la atribución de responsabilidad y toma de decisiones a nivel político y militar. De este modo, la construcción de la estructura de la ciberdefensa depende de los conocimientos de gestión de operaciones cibernéticas en un entorno de incertidumbre, debido a que las nuevas amenazas y los actores que surgen se caracterizan, siguiendo a Zygmunt Bauman, por fluir dentro del ciberespacio en tiempo y espacio y sus relaciones son matizadas por la influencia de intereses. Por lo tanto, los desafíos se encuentran, primero, en clasificar las amenazas que se renuevan constantemente debido al avance de la tecnología y segundo, en los agentes de amenaza que se mantienen en su mayoría en el anonimato. Esta situación ha creado un ambiente de incertidumbre y le agrega más complejidad a la interdependencia. Es así, que Ecuador tomó la decisión de estructurar la institucionalidad y políticas en pro de la ciberdefensa.

El estudio del estado del arte de la ciberdefensa en Ecuador permitió establecer que no existe una institución que centralice el tema, no obstante, el Ministerio de Defensa en cuanto políticas ha promulgado directrices sobre la información estatal como parte de la soberanía e integridad territorial. También, los esfuerzos de las Fuerzas Armadas a nivel operativo se evidencian en el Comando de Ciberdefensa, sin embargo, no existen registros de sus actividades, metodologías ni resultados. Paralelamente, se carece un marco jurídico especializado en operaciones cibernéticas, pero a través de COIP se aproxima a penalizar las amenazas cibernéticas. A pesar de todos los avances de Ecuador en ciberdefensa, éste no funciona de manera sistemática, ni coordina las diferentes instituciones en beneficio de la estructura estatal y de sectores estratégicos. De esta manera, ha condicionado la capacidad de la institucionalización en ciberdefensa.

El análisis del caso de estudio pone en evidencia la vulnerabilidad de los sistemas de información de las entidades públicas. De hecho, trasladar el sector público al dominio virtual expone la seguridad de la información estatal a ataques y amenazas cibernéticas y, profundiza las relaciones de poder. El gobierno ha publicitado la información a través de las TIC, con el objetivo de crear un espacio de interacción entre las instituciones y la ciudadanía. En este sentido, existe una relación entre el nivel de apertura y nivel de riesgo, que como resultado sino se

han establecido mecanismos de ciberdefensa, emergen ataques a las instituciones. Ecuador en el Plan Nacional de Gobierno Electrónico (2014-2017) ya presenta diversos portales y sistemas de la administración pública. Con relación a los esfuerzos realizados y proyectos transversales en las entidades públicas se han reconocido resultados, no obstante, existe diferentes niveles de madurez en la gestión y desarrollo de las TIC entre las diferentes instituciones.

El caso de la vulnerabilidad del sistema de la Senescyt se analiza a través de la tabla 4, con el fin de identificar los agentes de la amenaza y objetivos en el desarrollo de la operación cibernética. El análisis permite establecer el alcance, la magnitud y la complejidad del ataque. Además, se da seguimiento a las instituciones que intervinieron en el caso a través de una tabla general (5) en base a la propuesta de Choucri, Madnick y Koepe. El objetivo de la tabla permite medir a través de datos cuantitativos y cualitativos el desempeño de la organización.

En primera instancia, el análisis se realiza en base a los resultados de la investigación del operativo "Impacto Inicial". Por un lado, los agentes de la amenaza se consideran en la categoría de organización criminal, debido a que se estableció de manera legal que se trataba de una asociación ilícita, es decir, dos o más personas que se asocian con el objetivo de cometer delitos (art.370, COIP), en el caso se detuvieron a diez personas. Además, se catalogó como una red de *hackers* que operaba y trabaja coordinadamente en el ámbito nacional e internacional. Por otro lado, el objetivo se clasifica en la categoría de venta y publicación de información, pues se registraron títulos ilícitamente en el Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE), a cambio de remuneraciones económicas.

TABLA 5

ANÁLISIS DEL AGENTE DE AMENAZA Y OBJETIVO

Agente de la amenaza	**Sector Público**
Organizaciones Criminales	Publicación y venta de información
Caso Senescyt	
Asociación con el fin de cometer delitos	Publicación de títulos en el SNIESE

Fuente: Fiscalía General del Estado y Ministerio del Interior, 2016
Elaborado por: Cristina Salinas

En la tabla 5 se asignan las categorías ya expuestas en el párrafo anterior. En cuanto al código de colores se encuentra en el color amarillo, que tiene tres características. En un primer momento, se destaca que en general en el sector público no se encuentran nuevas amenazas o tendencias en relación a este tipo de operación cibernética. Seguidamente, en el ámbito de defensa y seguridad se destaca que se disponen las medidas e instrumentos suficientes para neutralizar el ataque o amenaza. Finalmente, en el período de análisis (2016) no se encuentran de manera global incidentes significativos. En efecto, se puede concluir que la vulnerabilidad del SNIESE se encuentra en la categoría de ataques cibernéticos de bajo riesgo. Lo anterior demuestra que, a pesar de acoplarse Ecuador a las nuevas estructuras que se forman a nivel global y configurar un sistema local en aras de la seguridad y defensa, se observa que existen vulnerabilidades al sistema en base un nivel bajo de complejidad. Es así, que la capacidad del Estado se cuestiona en base a la conducción político-estratégica de la defensa.

En relación a la metodología propuesta sobre el seguimiento de las instituciones se elabora la tabla 6, que tiene como propósito establecer las instituciones que intervinieron en el caso, igualmente, el análisis se centra en los resultados expuestos en el operativo “Impacto Inicial”. La respuesta de la vulnerabilidad del sistema se centra en cuatro entidades (Fiscalía General del Estado, Ministerio del Interior, Policía Nacional y Secretaría Nacional de

Administración Pública) y se analiza, su rol, la disponibilidad de datos en materia de ciberseguridad y ciberdefensa y ejemplo de variables que gestionan.

La tabla presenta cuatro columnas, las dos primeras, corresponden a las instituciones y la descripción de sus funciones. La tercera, recoge el resultado de la disponibilidad de los datos, en tres rangos: baja, moderada y alta. Los criterios de selección se establecen en la cuarta columna; así, se consideran desde publicaciones de boletines de prensa hasta estimaciones estadísticas. Los criterios en cuestión evalúan la calidad y cantidad la información e investigación en concordancia con el contexto del Estado ecuatoriano. De tal manera, se considera de rango bajo, notas y boletines informativos de actividades de la institución e investigaciones elaboradas por diferentes instituciones que centran su análisis a nivel global. En cuanto al rango medio, son datos secundarios, como estadísticas, reportes e información sobre la situación nacional. Finalmente, el rango alto presenta la coalición de datos de seguridad entre países, patrones del tráfico en el ciberespacio, publicaciones anuales de datos, informes de cumplimiento, predicciones y soluciones. Éste último no se encuentra presente, pues requiere un mayor grado de conocimiento y recursos por parte de los gobiernos.

TABLA 6

SISTEMA INSTITUCIONAL EN BASE AL CASO SENESCYT

Institución	Rol	Disponibilidad de datos	Ejemplo de variables (si procede)
Fiscalía General del Estado	Órgano autónomo de la Función Judicial que dirige la investigación pre-procesal y procesal penal.	Moderada	Estadísticas de delitos informáticos en base a denuncias receptadas, publicaciones sobre métodos de evitar incidentes
Ministerio del Interior	Institución rectora y coejecutora de la política integral de seguridad ciudadana y convivencia social pacífica.	Baja	Publicaciones en boletines de prensa sobre información institucional de capacitaciones e investigaciones, información tecnológica y avances sobre delitos cibernéticos.
Policía Nacional: Dirección General de Inteligencia	Organismo encargado de generar conocimiento permanente y actualizado en inteligencia y contrainteligencia policial, en el ámbito nacional e internacional en los niveles estratégicos y operacionales.	Baja	Publicaciones sobre tendencias y consejos en ciberseguridad, delitos informáticos e información institucional sobre la participación en cumbres de seguridad.
Secretaría Nacional de Administración Pública	Entidad que gestiona la eficacia institucional de las entidades que conforman la Administración Pública Central y que dependen de la Función Ejecutiva, evalúa el gobierno electrónico.	Moderada	Plan Nacional de Gobierno Electrónico (índices sobre gobernanza de internet, estadísticas sobre cultura digital y sistemas informáticos y portales), publicaciones de información institucional sobre temas de ciberseguridad.

Fuente: Fiscalía General del Estado (s.f.); Ministerio del Interior (s.f.); Policía Nacional (s.f.); Secretaría Nacional de Administración Pública (s.f.).
Elaborado por: Cristina Salinas

El análisis establece que las cuatro entidades nacionales tienen disponibilidad de datos que varían en función de la institución. La Fiscalía que lideró la investigación se encuentra en la categoría moderada pues registra estadísticas de delitos informáticos desde el 2009 al 2014 a nivel nacional,

adicionalmente, publicaciones sobre prevención. La Secretaría Nacional de Administración Pública se clasifica también en la misma categoría debido a su condición rectora del gobierno electrónico y su liderazgo en la elaboración del Plan, que presenta índices secundarios sobre gobernanza de internet, cultura digital e identifica sistemas informáticos y portales institucionales. Por otro lado, la Policía Nacional y el Ministerio del Interior se encuentran en la categoría baja porque limitan los datos y la información a boletines de prensa y publicaciones de gestión institucional.

Por otra parte, no hay esfuerzos en curso para alinear y estandarizar metodologías de análisis o informes. No obstante, es importante mencionar que la falta de datos sólidos se puede atribuir a elementos subyacentes como la dificultad de cuantificar datos cibernéticos debido a factores como: la ubicación geográfica, el objetivo de los ataques, el desarrollo tecnológico y la falta de normas, como resultado, existen disparidades en el diagnóstico y en la clasificación de los hechos cibernéticos (Choucri, Madnick, & Koepe, 2016). Además, las instituciones que intervinieron en el caso pertenecen al aparato estatal, por lo tanto, no se encuentra registro de la colaboración de instituciones internacionales, sin fines de lucro o el sector privado. Así mismo, son instituciones que responden a la ciberseguridad,

El censo de instituciones que intervinieron en el caso, presenta una estructura colaborativa limitada en cuanto a generación de datos que aporten en investigaciones futuras, y es indefinida en relación a las responsabilidades de cada institución para coordinar la ciberseguridad de los ataques cibernéticos. En torno al caso, se puede concluir que las instituciones enfocadas en ciberseguridad cumplieron su rol en base a sus funciones y especializaciones, sin embargo, al tratarse de un caso de clasificación baja de ataque y de disponibilidad de datos entre baja y moderadas, se concluye la información en relación al grado de vulnerabilidad tiene una respuesta tardía de las organizaciones, y se destacan en un tema posterior, que son las investigaciones. Por lo tanto, el estudio también demuestra que la vulnerabilidad, en concordancia con Keohane y Nye (1989), propone un punto de modificaciones estratégicas, con el fin de cambiar la situación.

En el escenario ambiguo del ciberespacio y la ciberdefensa, la ausencia de consenso técnico y metodológico limita el actuar de las instituciones en casos como el Sistema Nacional de Información de la Educación Superior del Ecuador. Los efectos, se encuentran en la opinión pública que genera inseguridad, aunque se encuentren diversos métodos de vigilancia e instituciones que a cargo de la ciberseguridad y ciberdefensa, se acerca a la paradoja que propone Bauman (2013) en el que, en comparación con otras generaciones, la generación actual percibe la sensación cotidiana de inseguridad a pesar de estar más protegida. Por otra parte, en este nuevo espacio la política se ve restringida por lo global del dominio, es así que, que el accionar de los gobiernos ante el temor de la gente se considera como ineficaz.

VII. CONCLUSIONES

El análisis de la presente disertación plantea que la hipótesis: las vulnerabilidades de la ciberdefensa en Ecuador, en el periodo 2013-2016, tendrían origen en la falta de medidas jurídicas, institucionales, y técnicas desde el mismo Estado ecuatoriano; que evidenciaría la ausencia de seguridad en la información estatal, se cumple en su totalidad. A continuación, se presentan las conclusiones obtenidas de la presente investigación que argumentan lo mencionado:

- La seguridad es un concepto que se encuentra en constante evolución debido a que se ha convertido en parte fundamental del desarrollo de los Estados. Ante esta premisa, la seguridad integral se establece como un concepto amplio, que enfrenta el desafío de lograr encontrar un equilibrio estratégico entre los diferentes ámbitos que se relacionan y que requieren directrices, espacios y prioridades de las diferentes áreas que componen la concepción. La importancia de las definiciones, deben pasar más allá del discurso, pues establecen lineamientos que permitirán la operatividad de lo conceptual a lo práctico, como en el campo del ciberespacio.

- La aproximación teórica a los términos seguridad y ciberespacio "a priori" encuentra la problemática en la transformación constante de este espacio no físico. Por un lado, la visión realista se acerca al aspecto político y militar, estableciendo la ciberdefensa desde una perspectiva de poder y, por otro lado, debido a las amenazas el constructivismo considera actores no estatales y diversos temas que se desarrollan a causa de las identidades que se forman. La ambigüedad que surge establece pautas para asignar al constructivismo las amenazas que se conforman socialmente y al realismo, el manejo estatal y la militarización del ciberespacio, enfocado en la soberanía de este espacio a través del poder.

- En consideración al marco teórico de la seguridad integral en Ecuador, se concibe al constructivismo como la base discursiva, pues plantea la seguridad en torno al ser humano y su contexto, es decir, la armonía que debe existir entre los individuos, el Estado y el medio ambiente. El

discurso al abarcar distintas temáticas tiene la ventaja de definir el objeto y la percepción de la amenaza. No obstante, concretar el discurso implica proteger los niveles en el que se desarrolla el ser humano, que requiere recursos y conocimientos por parte del gobierno e instituciones; así, comprende nuevos costos, y la dificultad reincide en emplear planes, proyectos, programas, etc.

- El Estado ecuatoriano a través de las iniciativas jurídicas, institucionales y políticas ha establecido lineamientos básicos sobre el ciberespacio y ciberdefensa. En este sentido, existen todavía limitaciones por la naturaleza cambiante de los actores y las amenazas, es decir, se ha avanzado, pero persisten problemas conceptuales, de recursos y de conocimientos que impiden que el potencial de cada una de las funciones se aproveche.

- En cuanto a la ciberdefensa, Ecuador ha estructurado una institucionalidad que ha posibilitado la generación de entidades como el Comando de Ciberdefensa y el conocimiento básico de la cultura digital por parte del gobierno, no obstante, la ausencia de un consenso técnico-metodológico queda en los pendientes por analizar y configurar como puntos de referencia para orientar la seguridad y la defensa vinculadas a las operaciones cibernéticas. En este sentido, el desarrollo del sistema internacional, no se replica en el ámbito local.

- En relación con lo anterior, el Sistema Nacional de Información de la Educación Superior del Ecuador se presenta como resultado de la conectividad, la interdependencia y la expansión del gobierno electrónico. La vulnerabilidad del sistema muestra los desafíos que enfrenta el Estado ecuatoriano en cuanto a estrategias de ciberdefensa, y cabe recalcar que las amenazas seguirán ampliándose debido a las tecnologías emergentes. Así mismo, se ha generado una serie de problemáticas como ciberespionaje, disrupción, desfiguraciones, entre otras, que han contribuido a la reflexión en los diferentes niveles de tomas de decisiones y a la opinión pública, sobre las esferas de seguridad en el ámbito de la

administración pública y al entorno de inseguridad de los datos e información estatal.

- Respecto a los planteamientos desarrollados, la minimización de la discusión de las amenazas a la seguridad estatal por desconocimiento o subestimación han limitado la participación de diferentes actores, en aportar conocimientos técnicos, metodologías, procesos, aspectos jurídicos y, asesoramiento en general, lo que supone condicionar la profundización del tema en términos estratégicos.

- A nivel metodológico existe limitadas fuentes de análisis del aspecto institucional de entidades pertenecientes al ciberespacio, debido a la compleja relación entre la transformación del dominio y el comportamiento de la sociedad y las instituciones formales. También, se presentan dificultades en cuantificar los datos, pues este dominio cambia en tiempo y espacio y, además existe divergencia en la clasificación de las actividades cibernéticas.

- La interdependencia compleja se concibe como una teoría de las relaciones internacionales que trae a debate elementos que no se consideran en modelos tradicionales. La teoría se centra en temas como la política internacional y el sistema global, desde el cambio de paradigma del actuar del Estado pues presenta nuevos actores, agenda y canales de conexión. A pesar de que menciona al individuo, no analiza su accionar en base a su identidad, es así, que limita el investigar la influencia en los escenarios en los que se acercan las diversas identidades a través de la tecnología al ciberespacio.

- Referente a la modernidad líquida al tratarse de una teoría sociológica presenta numerosos elementos de análisis, sin embargo, se destaca el factor líquido, su acercamiento al tiempo y espacio y el actuar de los individuos en respuesta a la tecnología. Además, el autor avanza con la investigación en diferentes áreas y se aproxima a la vigilancia líquida, que

presenta la susceptibilidad de la sociedad en base a estructuras formadas en beneficio de la seguridad. Este paradigma propone que diversos escenarios pueden modificarse, así, se puede concebir distintas tendencias y realidades.

VIII. RECOMENDACIONES

Una vez realizado el análisis y las conclusiones previamente, se realizan las siguientes recomendaciones:

- El Estado debido a las limitaciones en relación al conocimiento en procesos y sistemas, sería conveniente que se enfoque en la búsqueda de soporte internacional de países que han empleado y liderado estrategias, programas y planes y, que han materializado sus objetivos, es el caso de España, Reino Unido, Francia, entre otros. Además, es necesaria la cooperación internacional con el fin de desarrollar un enfoque coordinado contra las amenazas cibernéticas, considerando el carácter transfronterizo del ciberespacio. Igualmente, participar activamente en organizaciones y foros internacionales y regionales sobre ciberdefensa.

- Es necesaria la implementación de una entidad que centralice el accionar y permita una simbiosis entre las diferentes instituciones, con una gestión y política enfocada en una estructura coherente de la ciberdefensa y en los diferentes ámbitos que engloba.

- Se cree pertinente formular o proponer metodologías intergubernamentales sobre informes, datos estadísticos e información de ataques y amenazas cibernéticas a las entidades del Estado, con el fin de beneficiar investigaciones futuras. Adicionalmente, se cree conveniente realizar documentos estratégicos que recojan previsiones sobre estrategias de ciberdefensa.

- Se recomienda coordinar y canalizar iniciativas entre la administración pública, el sector privado, organizaciones no gubernamentales y actores de la sociedad civil en línea con las directrices nacionales e internacionales en torno a la ciberdefensa. Adicionalmente, socializar lineamientos generales sobre el ciberespacio y ciberdefensa a los servidores públicos y la ciudadanía.

- Es indispensable que se realice aproximaciones enfocadas no solo en los ataques o amenazas que surgen en el ciberespacio, sino también, en las oportunidades que ofrece este nuevo dominio. De esta manera, se lograrían romper asimetrías entre Estados y actores.

- En lo que, respecta a la academia, es necesario profundizar en la investigación sobre este tema, el entorno cambiante del ciberespacio presenta un nivel creciente de elementos y, la ciberdefensa se encuentra en un ámbito de incertidumbre que requiere el análisis continuo.

- En relación a la metodología institucional, se considera ahondar en el área de especialización de cada institución, este acercamiento permitirá comprender la organización y los instrumentos de cada área en respuesta a las operaciones cibernéticas.

- En cuanto al aspecto teórico, se recomienda el acercamiento desde la teoría constructivista, pues se considera que el tema de individualidades que se generan en este nuevo espacio, construyen diversas identidades que forman la estructura, los Estados y las instituciones.

LISTA DE REFERENCIAS

Libros

Albán, J. P. (2016). ¡Punir o no punir, esa es la cuestión! (el derecho penal ecuatoriano y la sociedad de la información). *Regulación de Internet y derechos digitales en Ecuador* , págs. 23-58. Editorial USFQ - Línea Juris Dictio

Antonopoulos, C. (2015). State responsability in cyberspace. En *Research Handbook on International Law and Cyberspace* (págs. 55-71). Edward Elgar Publishing Limited. Recuperado de https://books.google.com.ec/books?id=9ufECQAAQBAJ&pg=PA55&lpg=PA55&dq=thenotionalenvironmentin+which+digitized+information+communicated+over+computer+networks&source=bl&ots=yoix9Z0cKR&sig=IJ8AhteocPpJ6sOSQh4mUW8YJGE&hl=en&sa=X&redir_esc=y#v=onepage&q=then

Bauman, Z. (2002). *Modernidad Líquida.* Argentina: Fondo de Cultura Económica de Argentina S.A.

Bauman, Z., & Lyon, D. (2013). *Vigilancia Líquida.* Paidos Iberica

Buzan, B. (1991). People State and Fear: an Agenda for International Security Studies in the Post Cold War Era. Lynne Rieder.

Buzan. B, Wæver O & de Wilde J. (1998). Security: A New Framework For Analysis. Lynne Riennes Publishers.

Castells, M. (2001). La política de Internet. Privacidad y libertad en el ciberespacio. En M. Castells, *La Galaxia Internet* (págs. 166-193). Madrid: areté.

García, B. (2008). Seguridad y Defensa frente a la Asamblea Consituyente . En J. Echeverría, & C. Montúfar, *Plenos poderes y transformación constitucional* (pág. 205). Quito: Diagonal, capítulo Ecuador; Abya-Yala.

Gibson, W. (1989). Neuromante . En W. Gibson, *Neuromante* (pág. 35). Minotauro.

Keohane R. & Nye J. (1989). Power and Interdependence. Harvard Harper Collins Publisher

Lewis, J. A. (2012). Privacidad y seguridad en la red. La regulación y los mercados . En F. Telefónica, *Contribuciones para "Modelos reguladores de protección de datos para una era global"* (págs. 47-56). Madrid : Ariel, S.A.

Morgenthau, H. J. (1986). En H. J. Morgenthau, *Política entre las Naciones: La Lucha por el poder y la paz* (págs. 1-35). Bueno Aires : Grupo Editor Latinoamericano.

Pérez, J. (2008). *La Gobernanza de Internet. Contribución al Debate Mundial sobre la Gestión y el Control de la Red.* Madrid: Ariel.

Rojas, F., & Álvarez, A. (2012). Seguridad humana: Nuevos enfoques . *Seguridad Humana: Nuevos Enfoques*, 9-32. Recuperado de http://www.flacso.org/sites/default/files/Documentos/libros/secretaria-general/Seguridad%20Humana.pdf

Schäfer, P. J. (2012). The Concept of Security. En P. J. Schäfer, *Human and Water Security in Israel and Jordan* (págs. 5-18). Obtenido de Springer.

Stel, E. (2014). *Seguridad y Defensa del Ciberespacio.* Buenos Aires: Dunken. Recuperado de https://books.google.com.ec/books?id=H1lhAwAAQBAJ&pg=PA138&lpg=PA138&dq=el+ciberespacio+dentro+de+la+seguridad+estatal&source=bl&ots=rPJF7TtXtp&sig=JOJ8b1obLyILpAH1D67zk9gFJho&hl=en&sa=X&redir_esc=y#v=onepage&q=el%20ciberespacio%20dentro%20de%20la%20segur

Tejerina, O. (2014). *Seguridad del Estado y privacidad.* Madrid: Reus, S.A. Recuperado de https://books.google.com.ec/books?hl=en&lr=&id=dE6oBQAAQBAJ&oi=fnd&pg=PA9&dq=seguridad+y+privacidad+en+el+ciberespacio&ots=sEYBtmhJ-Y&sig=1jPmNt8N_Dd_o7XZz50BULUYBOs#v=onepage&q=seguridad%20y%20privacidad%20en%20el%20ciberespacio&f=false

Tsagourias, N. (2015). *The legal status of cyberspace*. Recuperado de Research Handbook on International Law and Cyberspace: https://books.google.com.ec/books?id=9ufECQAAQBAJ&pg=PA55&lpg=PA55&dq=thenotionalenvironmentin+which+digitized+information+communicated+over+computer+networks&source=bl&ots=yoix9Z0cKR&sig=IJ8AhteocPpJ6sOSQh4mUW8YJGE&hl=en&sa=X&redir_esc=y#v=onepage&q=cybe

Waltz, K. N. (1988). *Teoría de la Política Internacional.* Buenos Aires: Grupo Editor Latinoamericano.

Wolfers, A. (1952). National Security as an Ambiguous Symbol. Political Science Quarterly.

Documentos Legales

Código Orgánico Integral Penal . (2014). Recuperado de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Constitución de la República del Ecuador . (2008). Recuperado de http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2011). Recuperado de http://www.oas.org/juridico/pdfs/mesicic4_ecu_comer.pdf

Ley Especial de Telecomunicaciones . (2011). Recuperado de http://www.oas.org/juridico/pdfs/mesicic4_ecu_especial.pdf

Ley Orgánica de Telecomunicaciones. (2015). Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Ley Orgánica de la Defensa Nacional . (2009). Recuperado de http://www.defensa.gob.ec/wp-

content/uploads/downloads/2012/07/LEY_ORGANICA_DE_LA_DEFENSA_NACIONAL.pdf

Ley Orgánica de Transparencia y Acceso a la Información Pública . (2004). Recuperado de http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Ley de Seguridad Nacional , N.- 275 (1979). Recuperado de Flacso: http://www.flacsoandes.org/internacional/gobiernos_en_linea/ecuador/02ley_de_seguridad_nacional_ECUADOR.pdf

Ley de Seguridad Pùblica y del Estado . (2009). Recuperado de http://www.oas.org/juridico/pdfs/mesicic5_ecu_panel5_sercop_1.3._ley_seg_p%C3%BAblica.pdf

Tesis de grado

Universidades en Ecuador

Benalcazar, G. (2008). *Discursos de la Seguridad Nacional en el Ecuador* . Recuperado de Flacso: http://repositorio.flacsoandes.edu.ec/bitstream/10469/1172/4/TFLACSO-GBH2008.pdf

Castro, E. (2015). *Estudio Prospectivo de las Ciberdefensa en las Fuerzas Armadas del Ecuador.* Recuperado de ESPE: https://repositorio.espe.edu.ec/bitstream/21000/11583/1/T-ESPE-049543.pdf

Dávila, M. (2012). *Análisis de la Convivencia entre las diferentes generaciones: Baby Boomers. Generación X y Generación Y, en el sector público; caso Secretaría Nacional de Educación Superior, Ciencia, Tecnologia e Innovación (SENESCYT).* Recuperado de http://repositorio.uasb.edu.ec/bitstream/10644/3069/1/T1124-MDTH-Davila-An%c3%a1lisis.pdf

Espinoza, J., & Verdezoto, R. (2015). *El rol de las auditoría forense ante los nuevos delitos informáticos tipificaos en el actual código orgánico integral penal del Ecuador COIP, metodologías y herramientas a usar ante una evidencia digital"*. Recuperado de Universidad Politécnica Salesiana : https://dspace.ups.edu.ec/bitstream/123456789/10348/1/UPS-GT001274.pdf

Haro, P. (2010). *La Ley de Seguridad Nacional, Útil herramienta política. Desde el retorno a la democracia 1979, hasta la publicación de las políticas de defensa 2003.* Recuperado de Flacso: http://repositorio.flacsoandes.edu.ec/bitstream/10469/2440/4/TFLACSO-2010PHA.pdf

Moscoso, A. (2014). *Ecuador y Colombia. Caso de estudio "Conflicto Angostura 2008-2011" y la ruptura de la paz democrática ante la amenaza a la seguridad.* Recuperado de Uasb repositorio: http://repositorio.uasb.edu.ec/bitstream/10644/3865/1/T1378-MRI-Moscoso-Ecuador.pdf

Murillo, D. (2013). *La concepción de Keohane sobre los regímenes ambientales internacionales* . Recuperado de FLACSO: http://repositorio.flacsoandes.edu.ec/bitstream/10469/6127/2/TFLACSO-2013DCMB.pdf

López, P. (2016). *La evolución de la función de inteligencia dentro del contexto de la seguridad integral: análisis y perspectivas en su entendimieno y aplicación* . Recuperado de Insitituo de Altos Estudios Nacionales : http://repositorio.iaen.edu.ec/bitstream/24000/3828/1/TESIS%20MAESTRIA.pdf

Pilca, E. (2015). *La Universidad, Dispositivo de Selección: Reforma a la Educación Superior Ecuatoriana* . Recuperado de http://repositorio.flacsoandes.edu.ec/bitstream/10469/7710/2/TFLACSO-2015EPPP.pdf

Quintero, D. (2014). *Las políticas regionales sobre ataques informáticos y su incidencia en la vulnerabilidad de la defensa de la Unasur en el período 2009-2013.* Recuperado de IAEN: http://repositorio.iaen.edu.ec/bitstream/24000/3782/1/TESIS-DANIEL%20QUINTERO.pdf

Sánchez, C. (2015). *De la Doctrina de Seguridad Nacional a la Seguridad Integral en el Ecuador.* Recuperado de ESPE: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/11587/T-ESPE-049558.pdf?sequence=1&isAllowed=y

Torres, F. (2000). *Tiwintza. El fin de un conflicto. Pasado y presente del problema territorial Ecuador-Perú.* Recuperado de https://repository.unm.edu/bitstream/handle/1928/12940/Tiwinza%20el%20fin%20de%20un%20conflicto.pdf?sequence=1

Universidades fuera de Ecuador

García, J. (2015). *Control y Privacidad en el Ciberespacio.* Recuperado de Repositorio Universidad de Valencia : http://roderic.uv.es/handle/10550/50812

Gaviria, P. (2016). *Aplicación de la Metodolgía de Malware para el Análisis de la amenaza persistente (APT) "Poison Ivy".* Recuperado de Universidad Internacional de La Rioja : http://reunir.unir.net/bitstream/handle/123456789/4738/GAVIRIA%20%2C%20PABLO%20ANDRES.pdf?sequence=1&isAllowed=y

Llongueras, A. (2011). *La Ciberguerra; la guerra inexistente.* Recuperado de https://www.academia.edu/6182513/La_Ciberguerra_la_guerra_inexistente

Martínez, Y. (2005). *El enemigo olvidado: la ricina y su amenaza como arma biológica a los Estados Unidos*. Recuperado de Universidad de las Américas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/mes/martinez_p_yi/portada.html

Muñoz, B. (2005). *La corrupción como amenaza a la seguridad nacional tras la transición democrática en México.* Recuperado de Colección de Tesis Digitales,

Universidad de las Américas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/portada.html

Nobile, M. (2003). *México y la agenda contemporánea de seguridad internacional: un estudio sobre los alcances del uso del concepto de seguridad humana* . Recuperado de Universidad de las Américas de Puebla : http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/nobile_g_m/

Rivera, M. (2004). *Regimenes internacionales de agua dulce en América del Norte* . Recuperado de UDLAP: http://catarina.udlap.mx/u_dl_a/tales/documentos/mes/rivera_l_mg/capitulo1.pdf

Valencia, S. (2014). *Ciberdefensa y Ciberseguridad: Una Nueva Propiedad para las Naciones.* Recuperado de Universidad Militar de Nueva Granada: http://unimilitar-dspace.metabiblioteca.org/handle/10654/12937

Publicaciones

Artículo de periódicos

Agencia Pública de Noticias del Ecuador y Suramérica . (2014). *Acceso a Internet reduce brecha digital en Ecuador* . Recuperado de http://www.andes.info.ec/es/noticias/acceso-internet-reduce-brecha-digital-ecuador.html

Agencia Pública de Noticias del Ecuador y Suramérica . (2015). *Unasur prepara red defensiva a través de fibra óptica para enfrentar "ciberataques".* Recuperado de http://www.andes.info.ec/es/noticias/unasur-prepara-red-defensiva-traves-fibra-optica-enfrentar-ciberataques.html

Agencia Pública de Noticias del Ecuador y Suramérica . (2016). *El 40% de títulos obtenido ilegalmente mediante hackeo en Ecuador son del área de Derecho* . Recuperado de http://www.andes.info.ec/es/noticias/40-titulos-obtenido-ilegalmente-mediante-hackeo-ecuador-son-area-derecho-audio.html

Agencia Pública de Noticias del Ecuador y Suramérica. (2013). *Sistema informático electoral del Ecuador sufrió ciberataque desde un país del primer mundo.* Recuperado de http://www.andes.info.ec/es/noticias/sistema-informatico-electoral-ecuador-sufrio-ciberataque-pais-primer-mundo.html

Bravo, D. (2015). *Ecuador se muestra vulnerable a ciberataques.* Recuperado de El Comercio : http://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Duarte, J. (2015). *Desde ayer rige la LOT en el país: se crea la Arcotel.* Recuperado de Metro Ecuador : https://www.metroecuador.com.ec/ec/estilodevida/2015/02/19/ayer-rige-lot-pais-se-crea-arcotel.html

Ecuadorinmediato. (2016). *Caso 'Impacto Inicial': Se ratifica prisión preventiva para ciudadano procesado por emisión irregular de licencias.* Recuperado de https://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_u

ser_view&id=2818795531&umt=caso_impacto_inicial_se_ratifica_prision_preventiva_para_ciudadano_procesado_por_emision_irregular_licencias

El Telégrafo . (2016). *Gobierno de EEUU termina su papel de supervisor de internet.* Recuperado de http://www.eltelegrafo.com.ec/noticias/tecnologia/30/gobierno-de-eeuu-termina-su-papel-de-supervisor-de-internet

Expreso . (2016). *Un funcionario de la ANT entre 10 detenidos por falsificar documentos. La Senescyt da de baja 366 títulos falsos. La ANT anulará 600 licencias.* Recuperado de http://www.expreso.ec/historico/un-funcionario-de-la-ant-entre-10-detenidos-por-falsificar-documentos-HYGR_8802812

Gonzáles, M. (2017). *Proyecto de Ley para controlar redes sociales e Internet fue enviado por Correa a la Asamblea el 23 de mayo.* Recuperado de El Comercio : http://www.elcomercio.com/actualidad/rafaelcorrea-ley-control-redes-internet.html

Jácome, E. (2016). *Abogada de Chiriboga: 'Voy a demostrar en derecho que mi título es legal'.* Recuperado de El Comercio: http://www.elcomercio.com/deportes/abogada-luischiriboga-titulo-falso-defensa.html

La Hora. (2016). *4 sentenciados en caso de títulos falsos.* Recuperado de https://lahora.com.ec/noticia/1101927597/4-sentenciados-en-caso-de-tc3adtulos-falsos

La Hora. (2016). "*Impacto Inicial": 10 ciudadanos con prisión preventiva.* Recuperado de https://lahora.com.ec/noticia/1101903384/e28098impacto-iniciale28099-10-ciudadanos-con-prisic3b3n-preventiva

Ortega, J. (2015). *Cibermafias atacaron a 17 empresas ecuatorianas.* Recuperado de El Comercio: http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html#.WVks7gGGC0I.email

Ortiz, S. (2016). *La Fiscalía entregó dos listados con títulos falsos.* Recuperado de El Comercio : http://www.elcomercio.com/actualidad/fiscalia-falsificacion-titulos-senescyt-investigacion.html

Ortiz, S. (2016). *Supuestos hackers podrían recibir hasta cinco años de cárcel.* Recuperado de El Comercio : www.elcomercio.com/actualidad/hackers-senescyt-titulosfalsos-licencias-carcel.html

Artículos de revista

Aranda, G., Riquelme, J., & Salinas, S. (2015). La ciberdefensa como parte de la agenda de integración sudamericana. *Línea Sur*(9), 100-116.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*, 5-26.

Bartolomé, M. (2004). Redifiniendo la Seguridad Internacional Contemporánea. *Revista Política y Estrategia*(94), 9-26. Recuperado de http://www.oocities.org/mcbartolome/anepe94.html

Basabe, S., Pachano, S., & Mejía, A. (2010). La Democracia Inconlus: Derechos Fundamentales, Instituciones Políticas y Rendimientos Gubernamentales en Ecuador (1979-2008). *Revista de Ciencia Política, 30*(1), 65-85.

Berea, A. E. (2009). El Concepto de Seguridad Nacioal en las Estrategias de Seguridad Nacional . *Los nuevos Paradigmas de la Seguridad* , 9-20.

Betancourt, V. (2012). ¿Utopía o posibilidad de resistencia y transformación en la era de la sociedad desinformada de la información? *Revista Latinoamericana de Comunicación Chasqui* , 94-97.

Buzan, B. (2008). People, States & Fear: An Agenda for International Security Studies in the post- Cold Wae Era. *Revista Acedémica de Relaciones Internacionales*(9), 1-53.

Cano, J. J. (2010). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global* . Recuperado de http://52.0.140.184/typo43/fileadmin/Revista_119/Editorial.pdf

Castells, M. (1996). La era de la información. Economía, socieddad y cultura . *México siglo XXI, 1*. Recuperado de Economía, sociedad y cultura: http://herzog.economia.unam.mx/lecturas/inae3/castellsm.pdf

Cordero, F. (2015). Estado, Sociedad Civil y Defensa Cibernética. *Patria, Análisis Pólítico de la Defensa, 1*(4), 12-33.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

Cubides, J., & Garay, C. (2013). Hacia la construcción de un estado del arte de seguridad y defensa nacional en Colombia. *Revista Cientifica "General José María Córdova", 11*(11), 81-98.

Cujabante, X. (2009). La Seguridad Internacional: Evolución de un Concepto . *Revista de Relaciones Internacionales, Estrategia y Seguridad*.

Craigen, D., Diakun, N., & Purse, R. (2014). Defining Cybersecurity. T*echnology Innovation Management Review,* 13-21. Recuperado de https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

Díaz, J. (2010). La Ciberseguridad en el Ámbito Militar. En M. d. Defensa, *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio* (págs. 217-256).

Erazo, J. (2011). El hábil delincuente. *Programa Estudios de la Ciudad*(44), 4-9.

Esteinou, J. (2001). Internet y la transformación del Estado. *Revista Latina de Comunicación Social*(6), 21-34.

Galán, C. M., & Cordero, C. G. (2016). La cibersguridad pública como garantía del ejercicio de derechos. *Derechos & Sociedad*(47), 293-306.

García, B. (2008). Una Nueva Ley de Seguridad Nacional del Ecuador . *Democracia, Seguridad y Defensa* , 1-12.

Gartzke, E. (2013). The Myth of Cyberwar. Bringing War in Cyberspace. Back Down to Earth. *International Security, 38*(2), 41-73.

Griffiths, J. (2007). Seguridad Hemisfperica en América Latina Alcances y Proposiciones. *Revista Globalización, Competitividad y Gobernabilidad, 1*, 88-104.

Iriarte, E. (2006). Internet Governance, en el filo de la navaja. *Revista de Internet, Derecho y Política*, 41-52. Recuperado de http://www.uoc.edu/idp/3/dt/esp/iriarte.pdf

Jean, E. S. (2007). The Changing Nature of "International Security": The Need for an Integrated Definition. *Paterson Review, 8*, 1-12. Recuperado de http://www.iusafs.org/pdf/stjean.pdf

Keohane, R. (1998). International Institutions: Can Interdependence Work? *Foreign Policy*(110), 1-7.

Koch, S. (2015). La libertad en el ciberespacio: ciberseguridad y el principio del daño. *Revista Ensayos Militares, 1*(2), 85-98.

Møller, B. (1996). Conceptos sobre Seguridad: Nuevos Riesgos y Desafíos. *Desarrollo Económico, 36*(143), 769-792.

Moreira, R. (2014). Amenazas cibernéticas contra la Seguridad del Estado . *Revista INADE* , 17-21.

Nieto, V. (2014). Ciberdefensa: Imperiosa necesidad estratégica . *Revista Fuerzas Armadas* , 64-67.

Larenas, A. A. (2013). La confluencia entre estudios críticos de seguridad seguridad humana: las dinámicas de inclusión y superación. *Relaciones Internacionales*(23), 81-98.

Leal, F. (2003). La doctrina de seguridad nacional: materialización de la guerra fría en América del Sur. *Revista de Estudios Sociales. 15*, 74-87.

Lekanda, P. (2009). El conflicto territorial entre Ecuador y Perú por el Río Cenepa (1995): entre una mediación fallida y otra exitosa. *revista Pléyade*(4), 187-211.

Orozco, G. (2006). El concepto de la seguridad en la Teoría de las Relaciones Internacionales. *Revista CIDOB d'Afers Internacionals* , 161-180.

Orozco, G. (2006). El aporte de la Escuela de Copenhague a los estudios de seguridad. *Revista Fuerzas Armadas y Sociedad, 20*(1), 141-162

Polo, J. (2016). Los CERTs como herramientas de apoyo a la ciberdefensa en las Fuerzas Armadas . *Revista de Ciencias de Seguridad y Defensa* , 17-24.

Prieto, G. S. (2011). La Corte Penal internacional Analizada desde la Teoría de la Interdependencia Compleja. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 6*(1).

Restrepo, J. C. (2013). La globalización en las relaciones internacionales: Actores internacionales y sistema internacional contemporáneo. *Revista Facultad de Derecho y Ciencias Políticas, 43*(119), 625-654.

Satapathy, S, & Ranjan, R. (2015). Ethical Kacking, *International Journal of Scientific and Research Publications*, 5 (6).

Sosa, D. (2014). La Ciber Guerra, una nueva amenaza y preocupación para la Seguridad del Estado . *Revista INADE*, 86-91.

Tamayo, E. (2013). Ciberespionaje Global y América Latina . *Patria, Análisis Político de la Defensa* , 83-101.

Ullman R. (1983). Redifining Security. *International Security,8*(1).

Vargas, R., Recalde, L., & Reyes, R. P. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de Seguridad* (20), 31-45.

Vásquez, A. (2008). Zygmunt Bauman: Modernidad Líquida y Fragilidad Humana. *Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas*, 1-8. Recuperado de http://pendientedemigracion.ucm.es/info/nomadas/19/avrocca2.pdf

Velásquez, E. (2002). Historia de la Doctrina de la Seguridad Nacional. Convergencia-Ciencias Sociales, *27*, 11-39.

Zambrano, C., & Gudiño, D. (2013). Perspectivas de integración sudamericana en seguridad y defensa. *Línea Sur, II*(6), 63-79.

Zhang, G., & Jacob, E. K. (2012). Reconceptualizing cyberspace: "Real" places in digital space. *The International Journal of Science in Society, 3*(2), 92-102.

Entrevistas

Delgado, A. (25 de Julio de 2017). Gobernanza de Internet, Ciberseguridad y Ciberdefensa. (C. Salinas, Entrevistadora)

Zamora, B. (30 de Septiembre de 2017). Caso "Vulnerabilidad del SNIESE de la Senescyt". (C. Salinas, Entrevistadora)

Páginas Web

Álvarez, G. (2007). *Nuevas Amenazas y su Impacto en la Seguridad Interna: El Caso Chileno en Perspectiva Comparada* . Recuperado de Pontificia Univeridad Católica de Chile : https://www.academia.edu/5796509/Nuevas_Amenazas_y_su_Impacto_en_la_Seguridad_Interna_El_Caso_Chileno_en_Perspectiva_Comparada

Álvarez, D., & Vera, F. (2017). Ciberseguridad y derechos humanos en América Latina. En *Hacia un Internet libre de censura II. Perspectivas en América Latina* (págs. 37-63). Buenos Aires : Fundación Universidad de Palermo . Recuperado de http://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Anca, L. (2015). *La ciberdefensa: hacia el desarrollo de una interoperabilidad conjunta del teatro de operaciones* . Recuperado de El Repositorio Digital del Centro Educativo de las Fuerzas Armadas: http://www.cefadigital.edu.ar/bitstream/123456789/478/1/TFI%2001-2015%20ANCA.pdf

Asociación para el Progreso de las Comunicaciones. (2014). *Se organiza en Ecuador primer encuentro nacional sobre gobernanza de internet.* Recuperado de https://www.apc.org/es/news/se-organiza-en-ecuador-primer-encuentro-nacional-s

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace* . Recuperado de Electronic Frontier Foundation: https://www.eff.org/cyberspace-independence

Camps, P. (2016). *Ciberdefensa y Cibeseguridad: Nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito.* Recuperado de Centro de Altos Estudios Nacionales: http://www.calen.gub.uy/pdf/investigacion/2016-1-Ciberseguridad-Camps.pdf

Castells, M. (2014). *El impacto de internet en la sociedad: una perspectiva global.* Recuperado de BBVA: https://www.bbvaopenmind.com/wp-content/uploads/2014/03/BBVA-Comunicaci%C3%B3n-Cultura-Manuel-Castells-El-impacto-de-internet-en-la-sociedad-una-perspectiva-global.pdf

Centro Criptológico Nacional- CERT. (2016). *Ciberamenazas 2015/Tendencias 2016.* Recuperado de https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

Centro de Estudios para la defensa Nacional. (2015). *Ciberseguridad y Ciberdefensa.* Recuperado Recuperado de Universidad de Belgrano: http://www.ub.edu.ar/centros_de_estudio/cedef/13_diciembre_2015.pdf

Chávez, C. (2016). Evolución Teórica del Concepto de Seguridad Humana y su Institucionalidad en el Contexto Actual. *Academia de Guerra del Ejército, Boletín Académico*(1), 3-10. Recuperado de http://www.cedeejercito.mil.ec/images/produccion_academica/boletines/boletin_1.pdf

Choucri, N., Madnick, S., & Koepe, P. (2016). Institutions for Cyber Security: International Responses and Data Sharing Initiatives . Recuperado de https://pdfs.semanticscholar.org/9eeb/844d15373719cc59c659a09905ed85b1816e.pdf

Cortés, C. (2014). *La Gobernanza de Internet: La Trampa de las Formas* . Recuperado de CELE: http://www.palermo.edu/cele/pdf/CELE_GobernanzaDeInternet.pdf

Cumbre Mundial sobre la sociedad de la información. (2005). *Informe del Grupo de Trabajo sobre la Gobernanza de Internet.* Recuperado de The Internet Governance Forum : http://www.wgig.org/docs/WGIG-Report-Spanish.pdf

Defensoría del Pueblo Ecuador . (s.f.). *Misión.* Obtenido de Defensoría del Pueblo Ecuador : http://www.dpe.gob.ec/que-hacemos/

Delgado, A. (2014). *Gobernanza de Internet en Ecuador: Infraestructura y acceso* . Recuperado de http://delgado.ec/research/es/Gobernanza_Internet_Ecuador_2014.pdf

EcuCERT. (2014). *MIsión.* Recuperado de Centro de respuesta a incidentes informátios del Ecuador : https://www.ecucert.gob.ec/nosotros.html

Eissa, S. G., Gastaldi, S., Poczynok, I., & Tullio, M. E. (2012). *El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino.* Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

Freire, B. (2014). *La Ciberdefensa en el Contexto de la Agenda Política de la Defensa.* Recuperado de http://www.imaginar.org/taller/ciberdefensa/D1_02_agenda_defensa_bfreire.pdf

FLOK Society . (2014). *Encuentro Nacional de Gobernanza de Internet (Ecuador).* Recuperado de http://floksociety.org/2014/11/15/encuentro-nacional-de-gobernanza-de-internet-ecuador/

Ganuza, N. (2010). *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*. Recuperado de Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio: https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

Gómez, Á. (2012). El ciberespacio como escenario de conflictos. Identificación de las Amenazas. En Centro Superior de Estudios de la Defensa Nacional, *El Ciberespacio. Nuevo Escenario de Confrontación* (págs. 169-203). Recuperado de CESEDEN http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

ICANN. (s.f.). *¿Qué es la ICANN?* Recuperado de https://www.icann.org/es

Jarrín, O. (2008). Reforma de las Fuerzas Armadas en América Latina y el impacto de las amenazas irregulares . *Wodrow Wilson Center Reports on the Americas* , 69-96. Recuperado de http://www.flacsoandes.edu.ec/libros/digital/39772.pdf

Joyanes, L. (2010). *Introducción. Estado del arte de la ciberseguridad.* Recuperado de Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio: https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

Justribó, C. (2014). *Ciberdefensa: Una visión desde la Unasur* . Recuperado de VII Congreso del Instituto de Relaciones Internacionles: http://sedici.unlp.edu.ar/bitstream/handle/10915/44716/Documento_completo.pdf?sequence=1

Kahn, R. E. (1995). The Role of Government in the Evolution of the Internet. En *Revolution in the U.S. Information Infrastructure* (págs. 13-24). Washington D.C.: National Academy of Sciences . Recuperado de https://www.nap.edu/read/4944/chapter/3

Kuehl, D. T. (2014). *From Cyberspace to Cyberpower: Defining the Problem* . Recuperado de http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf

Laborie, M. (2011). *La evolución del concepto de seguridad*. Recuperado de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf

Libro Blanco de la Defensa Nacional. (2002). Recuperado de http://www.resdal.org/Archivo/ecu-libro-cap2.htm

Libro Blanco del Ecuador. (2005). Recuperado de https://www.oas.org/csh/spanish/documentos/libro_blanco_del_ecuador_2006.pdf

Llumá, D. (2014). *Seguridad Ciudadana en el Ciberespacio.* Recuperado de Universidad Nacional de San Martín : http://www.unsam.edu.ar/surglobal/seguridad-ciudadana-en-el-ciberespacio/

López, E. (2011). *La Doctrina de la Seguridad Nacional y la Intervención en Estados Soberanos: ¿Un instrumento de Intelegencia Estratégica?* Recuperado de Centro Argentino de Estudios Internacionales : http://www.caei.com.ar/sites/default/files/historia24.pdf

Malec, M. (2003). *Security Perception: Within and Beyond the Traditional Aproach* . Recuperado de Naval Postgraduate School : http://www.dtic.mil/dtic/tr/fulltext/u2/a417522.pdf

Mead, N. R., Hough, E. D., & Stehney, T. R. (2005). *Security Quality Requirements Engineering (SQUARE) Methodology.* Recuperado de http://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf

Merejo, A. (2007). *La República Dominicana en el ciberespacio de la Internet. Ensayo filosófico cibercultural y cibersocial (1995-2007).* Recuperado de http://www.educando.edu.do/Userfiles/P0001%5CFile%5CRD_ciberespacio_internet2.pdf

Ministerio Coordinador de Sectores Estratégicos . (2016). *Valore/Misión/ Visión*. Recuperado de http://www.sectoresestrategicos.gob.ec/valores-mision-vision/

Ministerio Coordinador de Seguridad. (2015). *Ministerio Coordinador de Seguridad y SERCOP denuncian vulneración al Sistema Nacional de Contratación Pública.* Recuperado de http://www.seguridad.gob.ec/ministerio-coordinador-de-

seguridad-y-sercop-denuncian-vulneracion-al-sistema-nacional-de-contratacion-publica/

Ministerio Coordinador de Seguridad Interna y Externa. (2008). *Agenda Nacional de Seguridad Interna y Externa: Hacia una nueva política de Seguridad Interna y Externa 2008*. Recuperado de https://www.slideshare.net/boblen/agenda-nacional-de-seguridad-interna-y-externa

Ministerio de Coordinación de Seguridad, (2011). *Plan Nacional de Seguridad Integral 2011-2013*. Recuperado de https://www.slideshare.net/veranada/plan-de-seguridad-integral-de-ecuador

Ministerio Coordinador de Seguridad, (2014). *Plan Nacional de Seguridad Integral 2014-2017*. Recuperado de http://biblioteca.gestionderiesgos.gob.ec/items/show/27

Ministerio de Defensa Nacional, (2011). *Agenda Política de la Defensa 2011-2013*. Recuperado de https://issuu.com/micsecuador/docs/agenda_pol_tica_de_la_defensa

Ministerio de Defensa Nacional, (2011). *Agenda Política de la Defensa 2014-2017*. Recuperado de http://www.defensa.gob.ec/wp-content/uploads/downloads/2014/06/Agenda-Politica-Defensa.pdf

Ministerio de Relaciones Exteriores y Movilidad Humana. (s.f.). *Misión, Visión y Valores* . Recuperado de http://www.cancilleria.gob.ec/valores-mision-vision/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2016). *Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021*. Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Plan-de-Telecomunicaciones-y-TI..pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (2016). *Las Telecomunicaciones en el Ecuador* . Recuperado de https://issuu.com/yadiraalejandra/docs/telecomunicaciones_vf.compressed_2_

Ministerio el Interior. (2014). *Operativo 'Tempestad' permitió desarticulación de banda que vulneraba sistemas informáticos.* Recuperado de http://www.ministeriointerior.gob.ec/operativo-tempestad-permitio-desarticulacion-de-banda-que-vulneraba-sistemas-informaticos/

Ministerio del Interior. (2016). *Desarticulada red de hackers que vulneraba sistemas de entidades bancarias y públicas.* Recuperado de http://www.ministeriointerior.gob.ec/desarticulada-red-de-hackers-que-vulneraba-sistemas-de-entidades-bancarias-y-publicas/

Molina, J. M. (2014). *Globalización, Ciberespacio y Estrategia. Especial consideración a la estrategia de a información.* Recuperado de Instituto Español de Estudios Estratégicos : http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO100-2014_Globalizacion-CIberseguridad-Estrategia_JMMolinaMateos.pdf

Montúfar, C. (2006). *La Agenda del Ecuador* . Recuperado de Flacso: http://www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=9344

NETmundial. (s.f.). *Inicio.* Recuperado de http://www.netmundial.org/es/inicio

Nye, J. S. (2010). *Cyber Power.* Recuperado de Belfer Center for Science and International Affairs : http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Organización de los Estados Americanos . (2013). *"El Acceso a la Información Pública, un Derecho para ejercer otros Derechos".* Recuperado de https://www.oas.org/es/sap/dgpe/concursoinformate/docs/CortosP8.pdf

Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and Implications*. Recuperado de ProQuest : http://search.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?pq-origsite=gscholar&cbl=396500

Paredes, D. (2016). Importancia de la Ciberdefensa en las Operaciones Militares y en la Seguridad y Defensa del Estado. *Academia de Guerra del Ejército, Boletín Académico*, 93-98. Recuperado de http://www.cedeejercito.mil.ec/images/produccion_academica/boletines/boletin_1.pdf

Pérez, J. (2015). La Gobernanza de Internet en España 2015. Madrid.Recuperado de http://boletines.prisadigital.com/Gobernanza_Internet_Spain_2015.pdf

Plata, A. R. (2010). *Ethical Hacking.* Recuperado de UNAM: https://www.seguridad.unam.mx/historico/documento/index.html-id=7

Pollitt, M. M. (1998). *Cyberterrorism - Fact or Fancy?* Recuperado de https://es.scribd.com/document/21173253/Mark-M-Pollitt-Cyber-Terrorism-Fact-or-Fancy

Peña, P. (2013). *¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos* . Recuperado de ONG Derechos Digitales : https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-internet-ebook.pdf

PNUD. (2011). *El enfoque de la seguridad humana desde tres estudios de caso.* Recuperado de Instiuto Interamericano de Derechos Humanos : http://www.iidh.ed.cr/multic/UserFiles/Biblioteca/IIDHSeguridad/11_2011/d31ae043-1976-4d83-86e9-35323eef3393.pdf

Ramírez, R. (2013). *Tercera Ola de Transformación de la Educación Superior en Ecuador. Hacia la constitucionalización de la sociedad del buen vivir.* . Recuperado de http://www.sciencespo.fr/opalc/sites/sciencespo.fr.opalc/files/Tercera-ola-de-transformaci%C3%B3n-de-la-educaci%C3%B3n-superior-en-Ecuador3.pdf

Rozalén, R. (2017). *Los ciberataques al sector público se duplicaron de un 7% en 2015 a un 14% en 2016.* Recuperado de http://www.channelbiz.es/2017/05/09/los-ciberataques-al-sector-publico-se-duplicaron-de-un-7-en-2015-a-un-14-en-2016/

Secretaría de Educación Superior, Ciencia y Tecnologpia e Innovación. (2015). *Informe de Rendición de Cuentas. Año Fiscal 2015*. Recuperado de http://www.senescyt.gob.ec/rendicion2015/assets/informe-de-rendici%C3%B3n-de-cuentas-2015.pdf

Secretaría de la Inteligencia . (2014). *Proyecto "Fortalecimiento de las infraestructuras tecnológicas y comunicaciones seguras para la gestión de inteligencia Fase II"*. Recuperado de http://www.inteligencia.gob.ec/wp-content/uploads/2015/07/FITYCSFASE2.pdf

Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación . (s.f.). *Registro de Titulos*. Recuperado de http://www.senescyt.gob.ec/registro-titulos/

Secretaría Nacional de la Administración Pública. (2013.). *Estatuto Orgánico por Procesos de la Senescyt*. Recuperado de http://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/04/Estatuto.pdf

Secretaría Nacional de Planificación y Desarrollo, (2009). *Plan Nacional del Buen Vivir 2009-2013: Construyendo un Estado Plurinacional e Intercultural*. Recuperado de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2012/07/Plan_Nacional_para_el_Buen_Vivir.pdf

Secretaria Nacional de Planificación y Desarrollo. (2012). *Sistema Nacional de Información de la Educación Superior del Ecuador* . Recuperado de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2012/08/Presentacio%C3%8C%C2%81n-de-Sistema-Nacional.pdf

Secretaría Nacional de Planificación y Desarrollo, (2013). *Plan Nacional del Buen Vivir 2013-2017*. Recuperado de http://www.buenvivir.gob.ec/versiones-plan-nacional

Secretaría Nacional de Planiicación y Desarrollo. (2015). *Plan Estratégico SENPLADES 2014-2017*. Recuperado de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2015/10/Plan-Estrategico-Senplades-2014-2017.pdf

Serrano, M. (2012). *El Plan Nacional de Seguridad Integral de la República del Ecuador*. Recuperado de Instituto Español de Estudios Estratégicos : http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI13-2012_PlanNacionalSegIntEcuador_MASM.pdf

Šulović, V. (2010). *Meaning of Security and Theory of Securitization*. Recuperado de Belgrade Centre for Security Policy: http://www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf

Stone, M. (2009). *Security According to Buzan: A Comprehensive Security Analysis*. Recuperado de Groupe d'Etudes et d'Expertise "Sécurité et Technologies": http://www.geest.msh-paris.fr/IMG/pdf/Security_for_Buzan.mp3.pdf

Theiler, O. (2011). *Nuevas amenazas: el ciberespacio.* Recuperado de Revista de la OTAN: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

Turiso, J. (2012). La Evaluación del conflicto hacia un nuevo escenario bélico. EL Ciberespacio. Nuevo Escenario de Confrontación. Recuperado de Monografías del CESEDEN: http://studylib.es/doc/5086949/el-ciberespacio.-nuevo-escenario-de-confrontaci%C3%B3n

Unión de Naciones Suramericanas . (2008). *Consejo de Defensa Suramericano (CDS).* Obtenido de http://www.unasursg.org/es/consejo-defensa-suramericano

Unión de Naciones Suramericanas. (2009). *El Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN)* . Recuperado de http://www.unasursg.org/es/consejo-suramericano-de-infraestructura-y-planeamiento

Unión de Naciones Suramericanas. (s.f.). *Historia.* Recuperado de Unasur: http://www.unasursg.org/es/historia

Vanella, R. (2015). *Centro de Estudios Estratégicos.* Recuperado de Universidad de las Fuerzas Armadas: http://cespe.espe.edu.ec/la-evolucion-del-concepto-de-seguridad-by-ricardo-vanella/

Vargas, C. (2011). El Gobierno Electrónico o e-Gobierno. *Uni-Pluri/Versidad, 11*(1). Recuperado de http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/BD9EB0AFF79442F705257C170009C981/$FILE/9711.pdf

Vélez, C. (2013). Hardware y software . *Gaceta electrónica*, Recuperado de http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/GacetaNoviembre2013/Paginas/Hardwareysoftware.aspx.

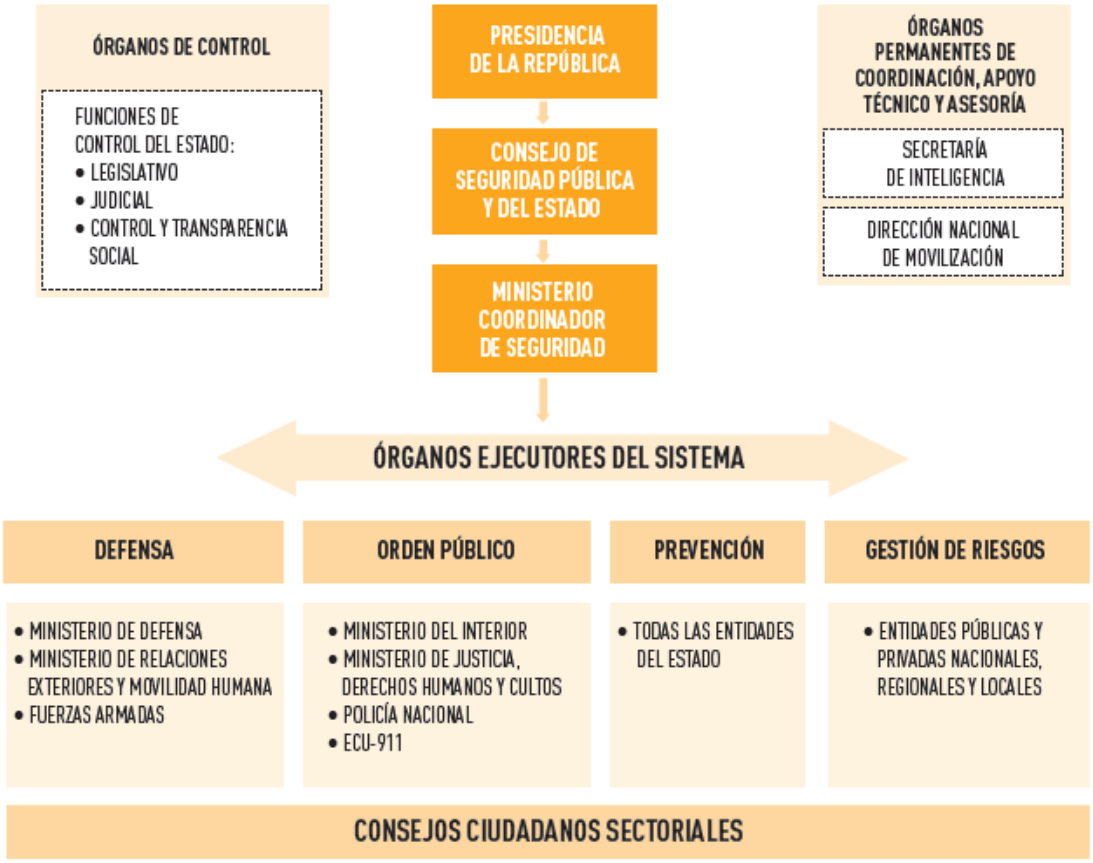
Vera, C., & Tamayo, F. (2010). *Gobernanza de Internet* . Recuperado de Internet Society : https://www.internetsociety.org/sites/default/files/pdf/538_20110119160126.pdf

ANEXOS

ANEXO 1: SISTEMA DE PLANIFICACIÓN PARA LA SEGURIDAD INTEGRAL

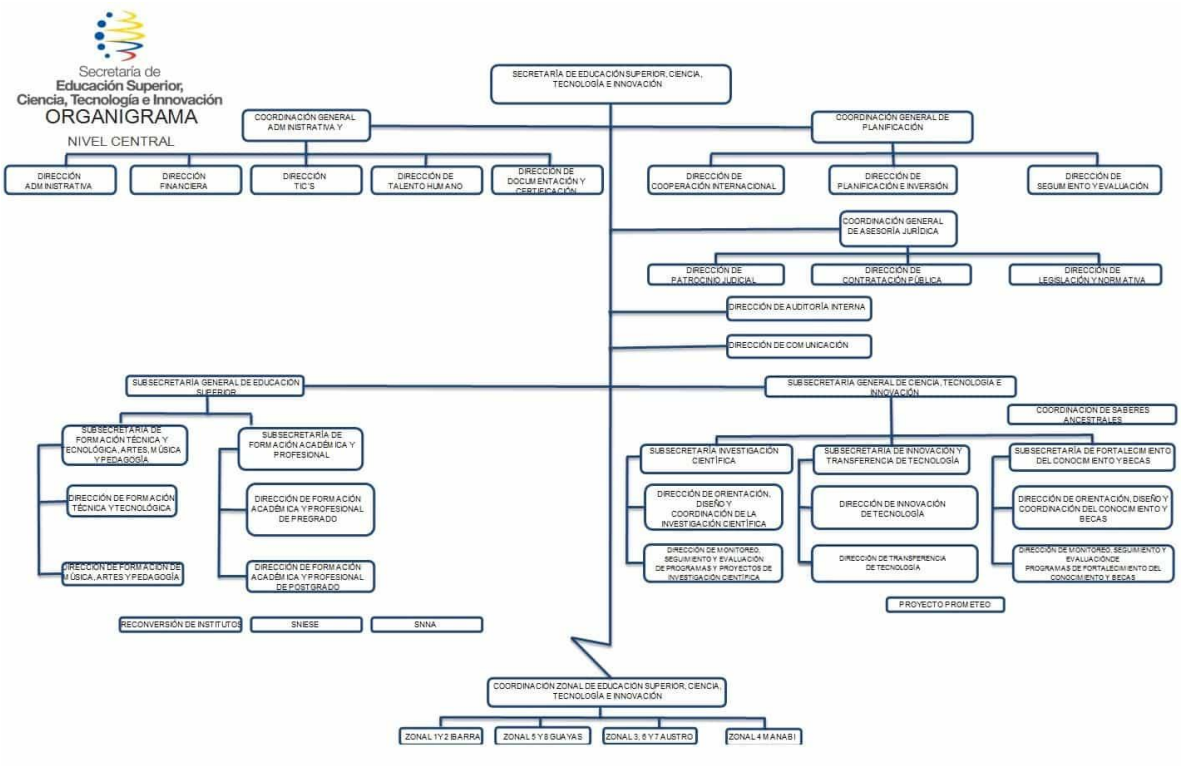
Fuente: Senplades, 2013
Elaboración: Ministerio Coordinador de Seguridad

ANEXO 2: SISTEMA Y ÓRGANOS DE SEGURIDAD PÚBLICA



Fuente: Plan Nacional de Seguridad Integral, 2011-2013
Elaboración: Ministerio Coordinador de Seguridad

ANEXO 3: ORGANIGRAMA DE LA SECRETARÍA DE EDUCACIÓN SUPERIOR, CIENCIA, TECNOLOGÍA E INNOVACIÓN



Fuente: Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, s.f.
Elaboración: Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

ANEXO 4: SISTEMAS INFORMÁTICOS Y PORTALES EXISTENTES

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Gestión Documental -Quipux		x	x			x	x	x				5
Gobierno por Resultados (GPR)				x		x		x				3
Portales Institucionales Homologados							x	x				2
Sistema de Inteligencia de Mercados				x				x				2
Sistema Único de Información Ambiental (SUIA)				x				x				2
Ventanilla única de Exportación (VUE)				x				x				2
Servicio de Turnos para Licencias de Conducción				x				x				2
Sistema de Consulta en Línea de Multas por infracciones de Tránsito (ANT)				x				x				2
Sistema de Emisión de licencias de conducir y consultas en línea para Discapacitados (ANT)				x				x				2
Sistema Integral de Información de Desarrollo Urbano y Vivienda (SIIDUVI)				x				x				2
Sistema de Información del Ministerio de Educación (SIME)				x				x				2
Sistema de Incentivos para Vivienda para Personas Migrantes				x				x				2

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Registro de comercializadores de bienes de producción nacional (SBPN)				x				x				2
Sistema de Registro Único del Ministerio de Industrias y Productividad.				x				x				2
Registro de producción Nacional de Bienes y Servicios (RPN-BS)				x				x				2
Sistema de Registro de Centros de Acopio y Recicladores (SIRCAR)				x				x				2
Sistema de Monitoreo de Importaciones del Ministerio de Industria y Productividad (SMIMIP)				x				x				2
Sistema de Registro de Reencauchadoras				x				x				2
Consulta de Antecedentes Penales				x				x				2
Sistema para Reclutamiento en Línea para aspirantes a Policía Nacional				x				x				2
Consulado Virtual				x				x				2
Socio Empleo				x				x				2
Sistema de Registro de Contratos en Línea				x				x				2
Sistema de Actas de finiquito en línea				x				x				2
Registro Social				x				x				2
Programa Postulación a Becas				x				x				2
Programa postulación Prometeo				x				x				2

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Sistema Registro de Títulos				x				x				2
Préstamos Hipotecarios				x				x				2
Préstamos Quirografarios				x				x				2
Servicios para Afiliados				x				x				2
Servicios para Jubilados				x				x				2
Servicios para Personas Naturales				x				x				2
Servicios para Personas Jurídicas				x				x				2
Sistema Nacional de Pagos				x				x				2
Servicios Bancarios Internacionales				x				x				2
Deposito Centralizado de Valores				x				x				2
Sistema Unitario de Compensación Regional de Pagos				x				x				2
Sistema de Cobros Interbancarios				x				x				2
Sistema de Cobros del Sector Público				x				x				2
Solicitud de Casillero Virtual				x				x				2
Solicitudes de Capacitación en Línea – SECAP				x				x				2
Capacitación Virtual – SECAP				x				x				2
Capacitación Virtual – IAEN				x				x				2
Datos Seguro				x				x				2

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Ventanilla Única Virtual (VUE)				x				x				2
E- Sigef				x				x				2
SPryn				x				x				2
Sistema Integrado de Planificación e Inversión Pública				x				x				2
Bus Gubernamental				x				x				2
InfoDigital				x				x				2
Sistema Nacional de Información Pública (SNI)				x				x				2
Portal de Trámite Ciudadano (PTC)								x				1
Automatización de contratos deportivos								x				1
Sistema Administración Deportiva								x				1
Catálogo Digital de Redes de Distribución de Energía Eléctrica								x				1
Sistema de Información Forestal (SAF)								x				1
Infraestructura de Datos Espaciales ambientales (IDEA)								x				1
Sistema de Información Nacional de Agricultura, Ganadería, Acuacultura y Pesca								x				1
Sistema Integral de Gestión Educativa Ecuatoriana (SIGEE)								x				1
Sistema de Integrado de Desarrollo Profesional Educativo (SiProfe)								x				1

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Registro Único de Actores Culturales Ecuador (RUAC)								x				1
Subsistema de Administración de Proyectos Culturales (SAPC)								x				1
Subsistema de Incentivos Ciudadanos para la Cultura (SICC)								x				1
Sistema para Seguimiento de Proyectos Deportivo								x				1
Pensiones Deportivas Vitalicias								x				1
Administración de Extensiones - Deportes								x				1
Director de Funcionarios - Deportes								x				1
Seguimiento de Convenios Deportivos								x				1
Documentación de Procesos – Deportes								x				1
Sistema Administración Deportiva								x				1
Programa de Formación Continua								x				1
Sistema de Gestión de Certificados de Origen (SIGCO)								x				1
Proyecto de renovación Industrial								x				1
Producepyme								x				1
Sistema de Salarios								x				1
Sistema de Información Nacional de Agricultura, Ganadería, Acuacultura y Pesca								x				1

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Sistema de Información de Biodiversidad								x				1
Sistema Nacional de Indicadores Ambientales								x				1
Sistema de Información Nacional Educativa								x				1
Portal de Ciclovías								x				1
Portal de Renovación Vehicular								x				1
Registro Interconectado de Programas Sociales								x				1
Sistema Consulta de Títulos								x				1
Tienda Virtual								x				1
Servicios de Impuestos en Línea (SRI)								x				1
Certificación Electrónica en Línea								x				1
SNP Cooperativas								x				1
Registro de Operadora de Regulación de Transporte Pesado								x				1
Formularios Electrónicos INEC								x				1
Ecuador en Cifras								x				1
Sistema Integrado de Consultas (REDATAM)								x				1
Consultas al Personal Encuestador INEC								x				1
Solicitudes en Línea de trámites IEPI								x				1
Sistema de Contratación Pública (SOCE)								x				1

Nombre Solución Existente	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Pasarela de Pagos								x				1
Gestión Vehicular Institucional								x				1
Sigen Integrador								x				1
Sistema Informático Integrado de Talento Humano								x				1
Postulantes - sorteo rural								x				1
SITOP								x				1
Sistema de Información para los Gobiernos Autónomos Descentralizados								x				1
CRM del Estado								x				1
Sistema de Contratación Pública (SOCE)								x				1
Sistema de Regulación Ambiental								x				1

Proyecto	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Proyecto 7	x	x	x	x	x	x	x	x	x	x	x	11
QUIPUX: Gestor documental nueva versión	x	x	x	x	x	x	x	x	x	x	x	11
EVEX Capacitación Virtual	x	x	x	x	x	x	x	x	x	x	x	11
Sistema de Automatización de procesos de prevención y control ambiental	x	x	x	x	x	x	x	x	x	x	x	11
Sistema de Talento Humano	x	x	x	x	x	x	x	x	x	x	x	11
Componente Integral de Aplicaciones Tecnológicas SRI	x	x	x	x	x	x	x	x	x	x	x	11
Identidad digital única	x	x	x	x	x	x	x	x		x	x	10
Portal de Software Público	x		x	x	x	x	x	x	x	x	x	10
Plataforma de Contacto Ciudadano	x		x	x	x	x	x	x	x	x	x	10
Observatorio de Gobierno Electrónico	x		x	x	x	x	x	x	x	x	x	10
Gestión de Conocimiento	x		x	x	x	x	x	x	x	x	x	10
Portal de Servicios Cloud	x		x	x	x	x	x	x	x	x	x	10
Portal de Documentación Legal	x		x	x	x	x	x	x	x	x	x	10
Portal de Gobierno Electrónico	x			x	x	x	x	x	x	x	x	9
Sistema de autoevaluación institucional	x	x	x	x		x	x	x		x	x	9
SNI Portal de Datos Abiertos	x			x	x	x	x	x	x	x	x	9
Contact Center del Estado	x			x	x	x	x	x	x	x	x	9

Proyecto	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Si Salud (Segunda fase)	x	x	x	x	x	x		x		x	x	9
Nuevo E-Sigef	x	x	x	x	x	x		x		x	x	9
Nuevo sistema de Pasaportes	x		x	x	x	x		x	x	x	x	9
Portal Gestión de Comunidades	x		x		x	x	x	x	x	x	x	9
Portal Versionamiento de codificación	x		x	x		x	x	x	x	x	x	9
Ventanilla Única Virtual (ciudadanía, empresas)	x		x	x		x	x	x	x	x		8
Gestión Educativa	x	x	x	x		x		x		x	x	8
Software Policía y Migración	x	x	x	x		x		x		x	x	8
Gestión Documental	x		x		x	x	x	x		x	x	8
Levantamiento, diseño y automatización del proceso de reforma institucional de la administración pública central, institucional y dependiente	x	x	x	x		x	x	x			x	8
Consulado Virtual		x	x	x		x	x	x			x	7
Portal Ecuador	x			x		x	x	x	x		x	7
Bus Gubernamental de Datos: autentificación y servicios web (segunda fase)	x		x	x		x	x	x		x		7
Sistema Integrad de los servivios y procesos de ANT	x	x		x		x	x	x		x		7
Pasarela de pagos	x	x	x	x		x		x		x		7

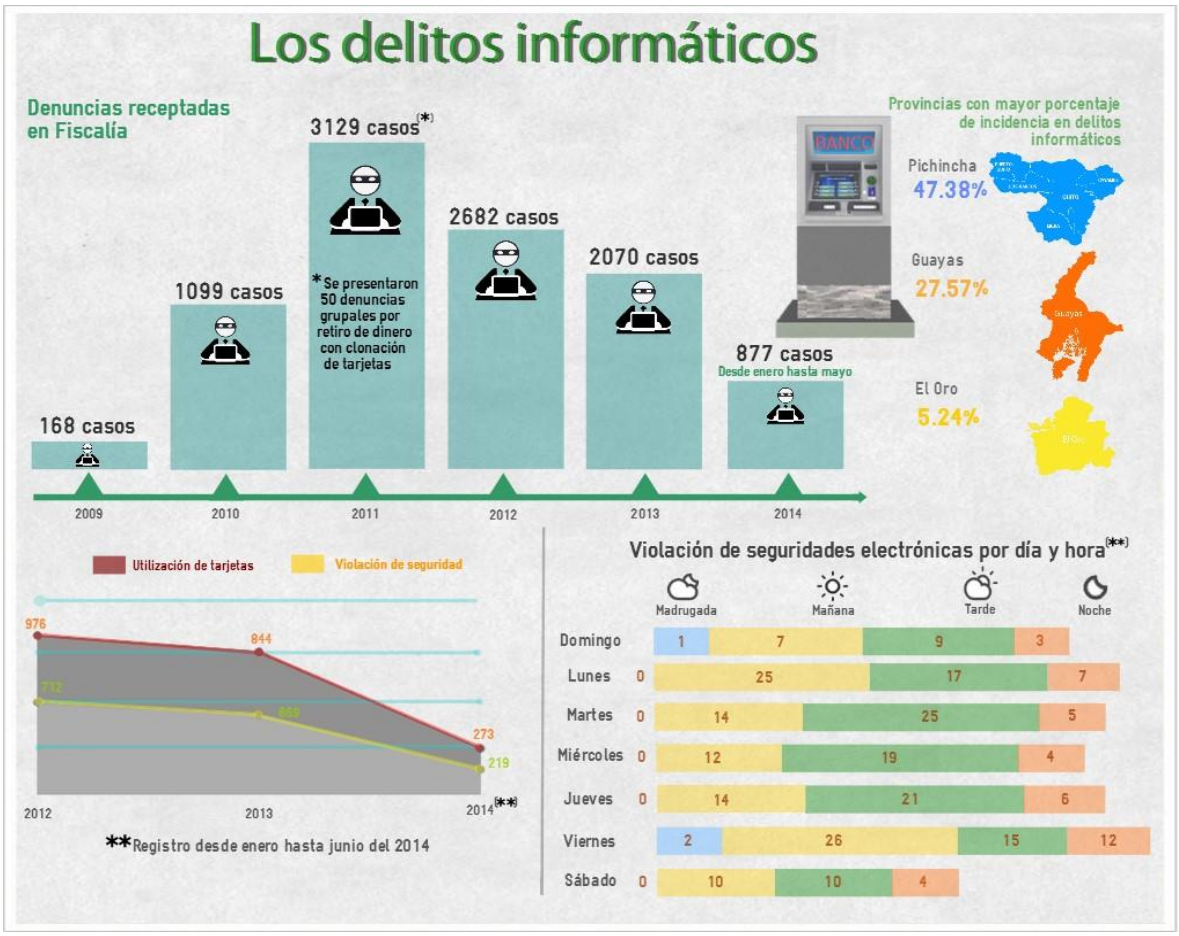
Proyecto	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Automatización de los macro procesos de auditoria minera	x	x	x	x		x	x	x				7
Bus de Datos Gubernamental servicios web (primera etapa)	x			x		x	x	x			x	6
Nuevo Sistema de Compras Públicas	x	x				x	x	x		x		6
Nueva versión de páginas Web homologadas	x			x	x	x	x	x				6
Automatización de procesos Adjetivos		x		x		x	x	x		x		6
Administración Centralizada de Usuarios y Permisos				x		x	x	x		x	x	6
Sistema de código postal en el ecuador a nivel de manzana	x		x	x		x	x	x				6
Consultoría para la implementación del sistema web mapa interactivo para el proyecto Amazonía viva	x				x	x	x	x	x			6
Trámite más engorroso	x			x			x	x			x	5
Si Salud (Primera fase)			x	x	x	x		x				5
Preguntas Quejas, Sugerencias y Felicitaciones	x			x		x	x	x				5
Plataforma de Seguridad de la Información	x					x	x	x		x		5
Digitalización de documentos				x			x	x		x	x	5

Proyecto	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Banco de información geológico del ecuador	x				x	x	x	x				5
Sistema que permite el acceso a la plataforma tecnológica -catálogo en línea- de fotografía patrimonial	x				x	x	x	x				5
Herramienta informática para la automatización de los procesos de medición de impacto de los Reglamentos Técnicos	x			x		x	x	x				5
Sistema integrador masivo de información de paquetería internacional en el sistema ecuapass	x			x		x	x	x				5
Centro de Servicios Compartidos – Servicios en la Nube	x			x		x		x				4
Sistema informático para el manejo, seguimiento, administración, evaluación y difusión, de información técnica generada	x					x	x	x				4
Software especializado para el tamizaje de cáncer colorectal CCR	x					x	x	x				4

Proyecto	Acceso Centralizado	Documentos electrónicos	Autenticación única	Interoperable	Esquema de datos abiertos	Contenidos de capacitación	Derechos y Patentes del Estado	Disponibilidad en la Nube	Mecanismos de participación	Mecanismos de evaluación	Accesibilidad y Usabilidad	Cobertura de Estrategias
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	Total
Ampliación de las capacidades del sistema de información para gestión de riesgos	x					x	x	x				4
Software de seguimiento para estrategia de mejoramiento del talento humano de los servicios de desarrollo infantil	x					x	x	x				4
Consolidación de las bases de datos de Registro Civil				x	x		x					3
Software en la plataforma tecnológica para el sistema nacional informático de donación y trasplante	x					x		x				3
Sistema de monitoreo vehicular exclusiva para el control de transporte de sustancias químicas controladas del sistema nacional de georeferenciación	x						x	x				3

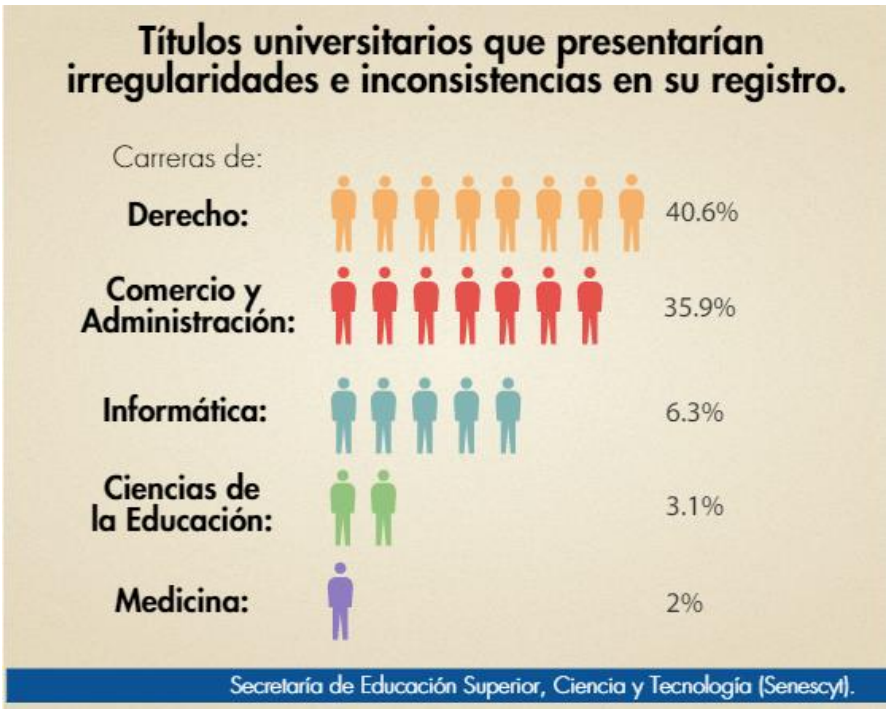
Fuente: Plan Nacional de Gobierno Electrónico, 2014-2017
Elaborado por: Secretaría Nacional de Administración Pública

ANEXO 5: LOS DELITOS INFORMÁTICOS



Fuente: Fiscalía General del Estado, 2014
Elaborado por: Fiscalía General del Estado

ANEXO 6: TÍTULOS UNIVERSITARIOS QUE PRESENTARÍAN IRREGULARIDADES E INCONSISTENCIAS EN SU REGISTRO



Fuente: Secretaría de Educación Superior, Ciencia y Tecnología, 2016
Elaborado por: Secretaría de Educación Superior, Ciencia y Tecnología